8/
mix

An Engineering Study of Onboard Checkout Techniques

A GUIDE TO ONBOARD CHECKOUT
VOLUME IV: PROPULSION

CR 115258

Huntsville

IBM

An Engineering Study of Onboard Checkout Techniques

A GUIDE TO ONBOARD CHECKOUT
VOLUME IV: PROPULSION

IBM NUMBER: 71W-00311

SEPTEMBER 1971

Prepared for the
National Aeronautics and Space Administration
Manned Spacecraft Center
Houston, Texas 77058

CONTRACT NUMBER NAS9-11189

IBM Federal Systems Division, Electronics Systems Center/Huntsville, Alabama

TABLE OF CONTENTS (Continued)

TABLE OF CONTENTS

TABLE OF CONTENTS (Continued)

FOREWORD

This is one of a set of seven reports, each one describing the results, for a particular subsystem, of a study titled "An Engineering Study of Onboard Checkout Techniques." Under the general title of "A Guide to Onboard Checkout," the reports are as follows.

Volume	IBM Number	Subsystem
I	71W-00308	Guidance, Navigation and Control
II	71W-00309	Environmental Control and Life Support
III	71W-00310	Electrical Power
IV	71W-00311	Propulsion
V	71W-00312	Data Management
VI	71W-00313	Structures/Mechanical
VII	71W-00314	R.F. Communications

This set of guides was prepared from the results of a nine month "Engineering Study of Onboard Checkout Techniques" (NAS9-11189) performed under NASA contract by the IBM Federal Systems Division at its Space Systems facility in Huntsville, Alabama, with the support of the McDonnell Douglas Astronautics Company Western Division, Huntington Beach, California.

Technical monitor for the study was Mr. L. Marion Pringle, Jr. of the NASA Manned Spacecraft Center. The guidance and support given to the study by him and by other NASA personnel are gratefully acknowledged.

Section 1

INTRODUCTION

1.1 OBJECTIVE

With the advent of large scale aerospace systems, designers have recognized the importance of specifying and meeting design requirements additional to the classical functional and environmental requirements. These "additional" requirements include producibility, safety, reliability, quality, and maintainability. These criteria have been identified, grown into prominence, and become disciplines in their own right. Presently, it is inconceivable that any aerospace system/equipment design requirements would be formulated without consideration of these criteria.

The complexity, sophistication and duration of future manned space missions demand that still another criterion needs to be considered in the formulation of system/equipment requirements. The concept of "checkoutability" denotes the adaptability of a system, subsystem, or equipment to a controlled checkout process. As with other requirements, it should also apply from the time of early design concept formulation.

The results of "An Engineering Study of Onboard Checkout Techniques" and other studies indicate that for an extended space mission onboard checkout is mandatory and applicable to all subsystems of the space system. In order to use it effectively, "checkoutability" should be incorporated into the design of each subsystem, beginning with initial performance requirements.

Conferences with researchers, system engineers and subsystem specialists in the course of the basic Onboard Checkout Techniques Study revealed an extensive interest in the idea of autonomous onboard checkout. Designers are motivated to incorporate "checkoutability" into their subsystem designs but express a need for information and guidance that will enable them to do so efficiently.

It is the objective of this report to present the results of the basic study as they relate to one space subsystem to serve as a guide, by example, to those who in the future need to implement onboard checkout in a similar subsystem. It is not practicable to formulate a firm set of instructions or recipes, because operational requirements, which vary widely among systems, normally determine the checkout philosophy. It is suggested that the reader study this report as a basis from which to build his own approach to "checkoutability."

1.2 BASIC STUDY SUMMARY

1.2.1 STUDY OBJECTIVE

The basic study was aimed at identification and evaluation of techniques for achieving the following capabilities in the operational Space Station/Base, under control of the Data Management System (DMS), with minimal crew intervention.

- Automated failure prediction and detection
- Automated fault isolation
- Failure correction
- Onboard electronic maintenance

1.2.2 STUDY BASELINE

The study started in July 1970. The system design baseline was established by the Space Station Phase B study results as achieved by the McDonnell-Douglas/IBM team, modified in accordance with technical direction from NASA-MSC. The overall system configuration was the 33-foot diameter, four-deck, 12-man station. Individual subsystem baseline descriptions are given in their respective "Guide to Onboard Checkout" reports.

1.2.3 STUDY TASKS

The basic study comprised five tasks. Primary emphasis was given to Task 1, Requirements Analysis and Concepts. This task established subsystem baseline descriptions and then analyzed them to determine their reliability/maintainability characteristics (criticality, failure modes and effects, maintenance concepts and line replaceable unit (LRU) definitions), checkout strategies, test definitions, and definitions of stimuli and measurements. After software preliminary designs were available, an analysis of checkout requirements on the DMS was performed.

A software task was performed to determine the software requirements dictated by the results of Task 1.

Task 3 was a study of onboard electronic maintenance requirements and recommendations of concepts to satisfy them. Supporting research and technology tasks leading to an onboard maintenance capability were identified. The study implementation plan and recommendations for implementing results of the study were developed in Task 4. The task final report also summarizes results of the study in all technical tasks.

Reliability, Task 5, was very limited in scope, resulting in an analysis of failure modes and effects in three Space Station subsystems, GN&C, DMS (computer group) and RF communications.

1.2.4 PREVIOUS REPORTS

Results of the basic study were reported by task in the following reports, under the general title of "An Engineering Study of Onboard Checkout Techniques, Final Report."

IBM Number	Title
71W-00111	Task 1: Requirements Analysis and Concepts
71W-00112	Task 2: Software
71W-00113	Task 3: Onboard Maintenance
71W-00114	Task 4: Summary and Recommendations
71W-00115	Task 5: Subsystem Level Failure Modes and Effects

Section 2

BASELINE SUBSYSTEM DESCRIPTIONS

2.1 GENERAL

This section describes the baseline Propulsion Subsystem which was analyzed to define onboard checkout requirements. In order to assess requirements for onboard checkout, descriptions at the subsystem level and the assembly level are required, as well as the major interfaces between subsystems.

The assembly level description for each of the subsystems (MSFC-DRL-160, Line Item 13) provided the primary working document for subsystem analysis. To reduce documentation, these documents have been incorporated by reference into this report, where applicable. Therefore, where no significant differences exist from the Phase B definition, this report contains a brief subsystem description and an identification of the referenced document containing the assembly level descriptions for that subsystem. Where significant differences do exist, the subsystem level description includes these changes in as much detail as is available. MSFC-DRL-160, Line Item 19, provided the major subsystem interface descriptions for analysis of integrated test requirements.

2.2 SUBSYSTEM LEVEL DESCRIPTION

The Space Station Propulsion System is required to perform the following functions:

- Provide attitude control, maneuvers, and docking functions prior to initial operations
- Perform spin/despin maneuvers for the artificial-g experiments
- Provide attitude control (wobble damp) during artificial-g experiment periods
- Perform orbit-keeping
- Provide control during docking maneuvers
- Provide backup attitude control

To accomplish these functions, a two-system propulsion subsystem was selected. A low-thrust, resistojet thrustor system using biowaste gases (CH_4, CO_2) as propellant will perform orbit-keeping and can, if desired, desaturate the CMGs. All other functions will be performed by a high-thrust, monopropellant hydrazine (N_2H_4) system.

The use of a biowaste resistojet system for orbit-keeping minimizes resupply, provides a useful method of biowaste disposal, minimizes contamination, and produces a near zero-g acceleration. A hydrazine high-thrust system for high torque, high impulse functions minimizes contamination and maximizes ease of maintenance.

The large quantities of propellant required for spin/despin maneuvers (6250 pounds per maneuver) prohibits initial loading, which necessitates resupply capability to be included in the design. This resupply can best be accomplished by bulk fluid transfer from the Advanced Logistic System (ALS) cargo module.

The Low-Thrust Propulsion System consists of five major assemblies:

- Collection and Storage Assembly
- Water Supplement Assembly
- Propellant Flow Control and Selection Assembly
- Thruster Assembly
- Power Distribution and Control Assembly

The High-Thrust Hydrazine Subsystem consists of seven major assemblies or assembly groups:

- High Presssure Storage Assemblies
- Pressure Control Assembly
- Propellant Tankage Assemblies
- Thruster Modules
- Resupply Assemblies
- Purge/Cleaning Assembly
- Propulsion Fault Isolation and Detection Assemblies

2.3 ASSEMBLY LEVEL DESCRIPTION

Descriptions of the Propulsion Subsystem assemblies and assembly groups are provided in the Space Station MSFC-DRL-160, Line Item 13, Volume I, Book 4, Utility Services. These descriptions include discussions of the major assemblies and assembly groups, block diagrams and drawings, and interfaces. DRL 13, Volume I, Book 2, is incorporated by reference into this report as a detailed description of the Propulsion Subsystem major assemblies and will become the primary working document for further analysis.

Section 3

RELIABILITY AND MAINTAINABILITY ANALYSES

3.1 CRITICALITY ANALYSIS

As a guide to emphasis in subsequent checkout technique studies, an analysis has been made of the overall subsystem and major component criticality (failure probability) of the Space Station subsystems and equipment. As an input to the Checkout Requirements Analysis Task, this data along with the failure mode and effects data will be useful in determining test priorities and test scheduling. Additionally, this data will aid in optimizing checkout system design to ensure that confidence of failure detection is increased in proportion to added system complexity and cost.

3.1.1 CRITICALITY ANALYSIS PROCEDURE

A criticality number (related to failure probability) was generated for each major subsystem component. This number is the product of: (1) the component failure rate (or the reciprocal of mean-time-between-failure), (2) the component's anticipated usage or duty cycle, and (3) an orbital time period of six months, or 4,380 hours. Six months was chosen as the time period of interest to allow one missed resupply on the basis of normal resupply occurring at three-month intervals. The criticality number, then, is the failure expectation for a particular component over any six-month time period.

For visibility, the major components of each subsystem analyzed have been ordered according to the magnitude of their criticality numbers. This number, however, should not be considered as an indication of the real risk involved, since it does not take into account such factors as redundant components, subsystem maintainability, and the alternate operational procedures available.

Overall subsystem criticality has been determined by a computerized optimization process whereby spares and redundancy are considered in terms of a trade-off between increased reliability and weight. This determination, therefore, reflects not only the failure probability of subsystem components, but also the probability that a spare or redundant component may not be available to restore the subsystem to operational status. The methodology used is described in Section 9, Long-Life Assurance Study Results, DRL 13 (Preliminary Subsystem Design Data), Volume III (Supporting Analyses), Book 4 (Safety/Long Life/Test Philosophy) from the MDAC Phase B Space Station Study. Component-level failure mode and criticality data are presented in subsequent paragraphs.

3.1.2 SUBSYSTEM CRITICALITY DATA

The Propulsion Subsystem six-month reliability prediction with 600 pounds of spares is 0.992. The two independent low thrust systems with inherent replacement capability of many critical components provide a high degree of assurance that orbit-keeping functions will be sustained for a ten-year period. No single or credible combination of failures can cause loss of the Propulsion System.

The criticality ranking of Table 3-1 indicates that the two-stage CO_2 and CH_4 pumps are the most critical. An additional spare unit may qualify here and greatly reduce the overall risk of failure.

3.2 FAILURE EFFECTS ANALYSIS

Based upon the baseline subsystem descriptions, each major subsystem component was assessed to determine its most probable failure mode(s), and the "mission effect" associated with this failure mode(s). The "mission effect" is noted to provide a brief explanation of Space Station behavior if the particular failure mode should occur (e.g., experiments degraded, crew hazard, etc.). The explanation generally does not, however, consider the offsetting effects of backup redundancy or spares since there would be practically no effect if these factors were considered.

In addition, the effect of failure is categorized into the following criticality classes:

(a) Category I - Failure could cause a loss of life.

(b) Category II - Failure could cause the loss of a primary mission objective.

(c) Category III - Failure could cause the loss of a secondary mission objective.

(d) Category IV - Failure results in only a nuisance.

In most cases, Category II and Category III failures are not distinguishable because primary and secondary mission objectives have not been identified to the level of detail required to permit such separation.

Examples of component level failure mode and criticality classification data are shown in Table 3-2, which is a partial listing.

Table 3-1. Propulsion Subsystem Criticality Ranking

Component	Single Unit Criticality (10^{-6})	Conditioned Loss Criticality (10^{-6})	Remarks
Pump and Motor	166,000	9,500	This numeric applies to both CO_2 and CH_4 pumps. Considers backup 2-stage pumps as nonoperating until required
Power Control Assembly	43,800	20	Internal redundancy plus backup
GN_2 Purge Tanks	42,000	180	Backup N_2 aboard S/S
Propellant Tank Assembly	42,000	2,000	Operation allowed with 11 of 14 tanks
Thruster Modules	13,700	75	Considers backup for despin and docking disturbance
Regulators	12,300	144	Applies to CO_2 and CH_4 regulators w/backup
Pressure Regulator (GN_2)	12,300	144	Backup failure considered
Relief Valves	8,900	16	Considers risk of GN_2 tank overpressurization
Burst and Relief Valve	8,900	56	Considers risk of propellant tank overpressurization

Table 3-1. Propulsion Subsystem Criticality Ranking (Continued)

Component	Single Unit Criticality (10^{-6})	Conditioned Loss Criticality (10^{-6})	Remarks
H_2O Tank	5,900	<10	Backup tank plus alternate source of CH_4 and CO_2 available
Accumulator (CH_4)	5,900	<10	Backup accumulator plus CH_4 can be obtained directly from EC/LS
Accumulator (CO_2)	5,900	<10	Backup accumulator plus CO_2 can be obtained from EC/LS
Valve Solenoid CO_2 Line to Accumulator	3,160	1	Backup plus EC/LS furnished CO_2 available
Valve Solenoid CH_4 Line to Accumulator	3,160	1	Backup plus EC/LS furnished CH_4 available
Regulation Valves	3,160	<10	Backup exists
Cross Feed Valves	3,160	<10	Backup exists
Isolation Valves	3,160	<10	Backup failure considered
Isolation Valves	3,160	<10	Backup failure considered
Valve, Solenoid (H_2O Tank to Vaporizer)	2,960	<10	Backup failure considered

Table 3-1. Propulsion Subsystem Criticality Ranking (Continued)

Component	Single Unit Criticality (10^{-6})	Conditioned Loss Criticality (10^{-6})	Remarks
Water Vaporizer	1,120	<10	Backup failure considered
Manifold	1,120	<10	Backup failure considered
Thruster Assembly	700	<10	Backup failure considered
Tank, Storage GN_2 (3000 psia)	440	<10	Backup failure considered
Pressure Switch Hi/Low	220	<10	Backup failure considered
Burst Disk	150	<10	Backup failure considered
Water Tank Heater	88	<10	Backup failure considered
Filter	44	<10	Backup failure considered
Filter	44	<10	Backup failure considered
Fluid Resupply Connectors	Neg'l		

Table 3-2. Propulsion Subsystem

Major Subsystem Component	Failure Mode(s)	Mission Effect	Failure Category	No. of Units	(A) MTBF/Source Thousands of Hours	(B) Duty Cycle (%)	Criticality Unit (4380 hrs X B/A X 10^{-6})
Low Thrust							
1) Accumulator (CH_4)	Leakage, rupture	Performance degraded, partial loss of orbit-keeping capability; loss of flexibility to choose accumulators	II/III	1/(1)	745/(12)	100	5,900
2) Accumulator (CO_2)	Leakage Rupture	Performance degraded; partial loss of orbit-keeping capability; loss of CMG desaturation capability	II/III	1/(1)	745/(12)	100	5,900
3) Pump & Motor	Motor shorted; no output cavitation pump bearing binds	Performance degraded CO_2 & CH_4 not compressed	II/III	2/2 (CO_2) 2/(2) (CH_4)	26.4/(12)	100	166,000
4) Filter	(Saturated) open	Performance degraded; impurities not filtered from CH_4 line or CO_2 line (as applicable) causing contamination downstream	II/III	1/(1) (CO_2) 1/(1) (CH_4)	100,000/(12)	100	44

3.3 MAINTENANCE CONCEPT ANALYSIS

Maintenance concepts defined for Space Station subsystems are intended to facilitate their preservation or restoration to an operational state with a minimum of time, skill, and resources within the planned environment. Maintenance concepts, in general, are discussed in Section 7.

The Propulsion Subsystem design incorporates specific maintenance or related provisions to satisfy the provisions of the general Space Station maintenance policy. The subsystem is designed for shirtsleeve maintenance, whenever possible, and no EVA shall be required.

Maintenance removal and replacement are by components and/or assemblies; i.e., no component adjustment and/or disassembly of components are necessary.

No scheduled maintenance (remove and replace) is planned with the exception of filters. Critical failure modes have safeguards (backup/redundancy or automatic fault isolation) designed into the subsystem.

The need for removal and replacement is determined by evaluation of:

- Leak and functional checks
- Actual life history of component and/or assemblies
- Performance checks
- Past development results/history

Safety provisions and/or procedures for normal crew maintenance operations are provided; for example,

- Propulsion subsystem assemblies are housed/installed in unpressurized (pressurizable) compartments.
- Propellant leak detection capability is provided in the compartments.
- Decontamination/cleaning methods/procedures for "breaking" into the subsystem (i.e., propellant removal from lines, components, filters, tanks, etc.) shall be established.

Reliability shall not degrade below the design reliability established. The design reliability is provided by:

- Maintenance/replacement of components and assemblies to meet design reliability requirements over a ten-year period.

- Safety factors/working stress levels that satisfy ten years of operation/fatigue, creep, corrosion, etc., wherever practical.
- More redundancy and/or automatic fault isolation for critical malfunction which affect safety of operations. The safety design feature must allow a mission operation to be completed (degraded performance allowed). This also allows maintenance to be scheduled whenever it is required.

The subsystem maintenance and operational approaches listed above will normally provide an autonomous Propulsion Subsystem with the reliability and safety needed for a ten-year mission. These features allow a balanced subsystem design approach to be taken to obtain the high reliability and safety needed without excessive redundancy/backup and the resulting complexity, volume, and weight penalties.

3.4 LINE REPLACEABLE UNIT ANALYSIS

General guidelines and criteria for the definition of LRUs were established and these along with the maintenance philosophies reported in Section 3.3 were used to determine at what level line maintenance would be performed. For the Space Station Subsystems specific justification applicable to LRU selection for the particular subsystem under examination was derived from the guidelines and these justifications are presented along with the LRU listing. The "functional LRUs" were then considered in the light of the standard electronic packaging scheme and actual LRUs were defined and listed. The method employed and the results achieved are discussed for both cases in the following sections.

3.4.1 SPACE STATION SUBSYSTEMS

The definition of Line Replaceable Units (LRUs) is keyed to repairing subsystems in an in-place configuration with the LRU being the smallest modular unit suitable for replacement. General factors considered in identifying subsystem LRUs include: (1) maintenance concepts; (2) the component-level failure rates delineated in the criticality analyses; (3) the amount of crew time and skill required for fault isolation and repair; (4) resultant DMS hardware and software complexity; and (5) subsystem weight, volume, location, and interchangeability characteristics. Listings of LRUs and more specific justification for their selection follows.

Line replaceable units for the low thrust portion of the Propulsion Subsystem are listed in Table 3-3. High Thrust Propulsion Subsystem LRUs are listed in Table 3-4. Although considerable operational redundancy exists within the subsystem, the only elements that can be categorized as "standby redundant" are the low-thrust flow control assembly and the high-thrust pressure control assembly.

Table 3-3. Low-Thrust Propulsion

LRU	Quantity
Collection/Storage Assembly	
Compression Pump	4
Propellant Storage Bottle	4
Filter	4
Relief Assembly	4
Tank Isolation Valve	4
Control Valve Assembly	2
Low Pressure Mixing Valve	2
High Pressure Mixing Valve	2
Water Supplement Assembly	
Storage Bottle	2
Water Vaporizer	2
Thermal Control Assembly	2
Fill/Drain Valve	1
Tank Isolation Valve	2
Flow Control Valve	2
Pressure Control Valve Assembly	2
Flow Control Assembly	
Regulator Assembly	2
Regulator Isolation Valve Assembly	2
Cross-feed Valve Assembly	1
Thruster Assembly	
Module Isolation Valve	8
Thruster Assembly	8
Power Distribution and Control Assembly	1

Table 3-4. Hi-Thrust Propulsion

LRU	Quantity
Press Storage Assembly (3000 psia GN_2)	
Storage Sphere	2
Relief Valve	2
Burst Disk	2
Isolation Valve	2
Pressure Transducer	2
Temperature Transducer	2
Hi-Press Manifold	
Isolation Valve	3
Vent Valve	2
Pressure Transducer	2
Filter Assembly	2
Disconnect Assembly	1
Press Control Assembly	
Regulator	2
Isolation Valve	2
Press Switch (hi/lo)	4
Filter	2
Lo-Press Manifold	
Isolation Valve	2
Press Transducer	2
Vent Valve	1
Disconnect Assembly	1
Propellant Storage Assembly	
Prop Tanks (Metal Bellows)	2
Relief Valve	2
Burst Disk	2
Isolation Valves (Prop and Ullage)	4
Press Transducer	4
Temperature Transducer	4
Qty Gauging (Assembly/System)	2

Table 3-4. Hi-Thrust Propulsion (Continued)

LRU	Quantity
Propellant Manifold	
Isolation Valve	6
Fill Valve	1
Vent Valve	1
Purge Valve	1
Press Transducer	3
Filter Assembly	1
Prop Dump Assembly (Nonpropulsive Prop Decomposition)	1
Disconnect Assembly	1
Thruster Modules	
Thruster Assembly	12
Isolation Valve	10
Filter Assembly	4
Press Transducer (liquid)	10
Press Transducer (Comb Chamber)	12
Temperature Transducer (Comb Chamber)	12
Purge Assembly	
Press Sphere	2
Regulator	1
Isolated Valves	8
Press Transducers	4
Resupply Assembly (Station)	
Isolation Valve (Press and Props)	4
Umbilical Hoses	4
Disconnect Assembly	4
Filters	4
Miscellaneous Assembly (allocation)	
Heaters	50
Thermostats	50
Temperature Transducer	30
Piping Assembly	50

Table 3-4. Hi-Thrust Propulsion (Continued)

LRU	Quantity
Cargo Module Resupply Subsystem	
Press Resupply	
Storage Spheres	2
Relief Valve and Burst Disk Assembly	2
Isolation Valve	2
Regulator	2
Press Transducer	2
Temperature Transducer	2
Disconnect and Umbilicals	2
Propellant Resupply	
Prop Tanks	2
Isolation Valves	2
Relief/Burst Assembly	2
Press Transducer	2
Temperature Transducer	2
Disconnects and Umbilicals	2

Primary criteria used in the selection of Propulsion Subsystem LRUs were component packaging, replacement frequency, and crew time and skill requirements. Also considered were the factors of parts commonality, DMS and instrumentation impacts, and LRU usage within the subsystem. Each subsystem component was analyzed to determine first if replacement might be necessary and second, if necessary, the optimum level of replacement in terms of minimizing impacts upon both crew and equipment. In all cases, the LRU has been selected so that a redundant capability exists to allow subsystem operation with an LRU removed. Some performance degradation or partial loss of flexibility is, of course, permitted in this situation.

Except where components are packaged together to minimize mechanical joints and connections, most Propulsion Subsystem LRUs are individual components. Another exception is the power distribution and control assembly. Lower level replacement is anticipated for this LRU when more detailed design information becomes available.

Section 4

OCS CHECKOUT STRATEGIES

4.1 SUBSYSTEM CHECKOUT STRATEGY

Before further requirements analysis, it is necessary to develop a checkout strategy for all Space Station subsystems to meet checkout objectives, which can be summarized as follows:

- To increase crew and equipment safety by providing an immediate indication of out-of-tolerance conditions
- To improve system availability and long-life subsystems assurancy by expediting maintenance tasks and increasing the probability that systems will function when needed
- To provide flexibility to accommodate changes and growth in both hardware and software
- To minimize development and operational risks

Specific mission or vehicle-related objectives which can be imposed upon subsystem level equipment and subsystem responsibilities include the following:

- OCS should be largely autonomous of ground control.
- Crew participation in routine checkout functions should be minimized.
- The design should be modular in both hardware and software to accommodate growth and changes .
- OCS should be integrated with, or have design commonality with, other onboard hardware or software .
- The OCS should use a standard hardware interface with equipment under test to facilitate the transfer of data and to make the system responsive to changes.
- Failures should be isolated to an LRU such that the faulty unit can be quickly removed and replaced with an operational unit.

- A Caution and Warning System should be provided to facilitate crew warning and automatic "safing" where required.

- Provisions must be included to select and transmit any part or all of the OCS test data points to the ground.

To attain these objectives via the use of an Onboard Checkout System which is integrated with the Data Management System, checkout strategies have been developed which are tailored to each Space Station subsystem.

Special emphasis has been applied to a strategy for checkout of redundant elements peculiar to each subsystem. The degree to which each of these functions is integrated into the DMS is also addressed.

4.1.1 SPACE STATION SUBSYSTEMS

Each major Space Station subsystem was examined with respect to the required checkout functions. The checkout functions associated with each subsystem are identified and analyzed as to their impact on the onboard checkout task. The functions considered are those necessary to verify operational status, detect and isolate faults, and to verify proper operation following fault correction. Specific functional requirements considered include stimulus generation, sensing, signal conditioning, limit checking, trend analysis, and fault isolation.

4.1.1.1 Propulsion Subsystem

The Propulsion Subsystem consists of two major elements, one being the low thrust resistojet system and the other the high-thrust monopropellant Hydrazine System. Both systems interface with the GN&C Subsystem and the Data Management Subsystem for control. In addition, the low-thrust system interfaces with the EC/LS Subsystem for biowaste propellants.

4.1.1.1.1 Checkout Functions

Checkout functions associated with the Propulsion Subsystem include continuous monitoring of critical parameters, short interval limit and status checking, and longer interval periodic in-depth testing to ascertain overall system health. The continuously sampled parameters include storage tank, regulator outlet, and manifold pressures, biowaste compressor pump speed, and heat exchanger temperature. Other critical parameters, such as thruster head temperature and resistojet heater power, also require high rate monitoring, but only at selected times, i.e., during thruster operation. Less critical system parameters including valve positions, propellant quantities, and secondary pressures and temperatures are

checked on a low rate or as-required basis to verify system status. In-depth testing is performed on a scheduled periodic basis or inconjunction with fault isolation and includes functional tests of valves, regulators, pumps, and other active components. Fault isolation is accomplished by combinatorial analysis of operating conditions and by functional testing.

- Stimulus Generation - Functional testing and fault isolation of the Propulsion Subsystem utilize the normal operating controls, such as valve actuation commands to establish the desired test conditions and to initiate functions to be tested. No additional stimulus requirements have been identified.

- Sensing - The sensing requirements associated with the Propulsion Subsystem are contained in Appendix I of the Task 1 Final Report.

- Signal Conditioning - Signal conditioning is required for all sensor outputs which do not fall within the standard measurement capability of the Remote Data Acquisition Units. The exact quantity and type of conditioning channels required are dependent upon sensor selection. Parameters such as valve position and event measurements are normally implemented as directly compatible bilevel voltages and require no special conditioning.

- Limit Checking - There are two types of limit checking required by the Propulsion Subsystem. The first is the continuous limit checking required in the case of critical but relatively static parameters, examples of which are tank, regulator output and manifold pressures, and heat exchanger temperatures. Out-of-limit conditions in these parameters indicate the need for relatively expedient relief or corrective action such as pressure venting which, depending upon the circumstances, may be either manually or automatically initiated. A second class of limit checking is associated with dynamic functions to which significant limits apply only during certain operating conditions, such as during thruster firing. Examples include thruster heat temperature and chamber pressure. Detection of an out-of-limit condition in these cases generally dictates termination of the operation or switching to an alternate mode. It is apparent from the foregoing that the requirement exists for selectively enabling and disabling the limit check on various parameters.

- Trend Analysis - Trend analysis has potential benefit in predicting end of life for wearout items in the system. The most promising application is in association with the biowaste resistojet thrusters. These units operate at very high temperatures using corrosive propellants, and therefore must be replaced from time to time. Typical failure modes include corrosion of the electrical heating elements and erosion or blockage of the nozzles. Long-term analysis of thruster power consumption, temperatures, and pressures are expected to yield information indicative of such failures. Trend analysis of another form is utilized to keep track of propellant and pressurant usage in both the low-thrust and high-thrust systems as an aid to controlling resource utilization and resupply operations.

4.1.1.1.2 Redundant Element Checkout

Redundancy in the low-thrust system is provided by two parallel systems from the EC/LS interface to the thrusters. These parallel systems each contain the valving, compression pumps, regulators, and storage tanks necessary to allow independent operation. Cross feeds and isolation valves are provided to allow interconnection of the two systems at various points if desired. This design also allows the two systems to be checked out and operated independently and allows bypassing or isolation of defective components for purposes of repair or replacement. The thrusters feature functional redundancy in that multiple thrusters or thruster pairs are capable of supplying any desired moment to the vehicle. These multiple units are also capable of independent checkout. Checkout of the redundant elements is therefore readily accomplished and presents no unique problems.

The high-thrust system also features redundancy in the form of multiple storage tanks, pressure regulators, and thrusters. The storage tanks and thrusters are isolatible by valving and may be exercised independently. The High Pressure Nitrogen Regulation System contains parallel regulators, one primary and one on standby, with automatic switchover via pressure switch interlock. Switchover to the secondary regulator may also be initiated by command, thus enabling checkout of the backup unit.

4.1.1.1.3 Integration with Data Management System

The checkout interface between the Propulsion Subsystem and the DMS consists of the measurement parameters listed in Appendix I. All measurements at the interface are in the form of normalized 0-20 mVdc, 0-5 Vdc, or 0-28 Vdc. No special test stimuli are required. Test sequencing and control as well as operational control and display, are provided by the DMS.

4.2 INTEGRATED CHECKOUT STRATEGY

This analysis identifies the integrated checkout functions associated with Space Station subsystems during the manned orbital phase of the mission. These functions are depicted in Figure 4-1 and are those required to ensure overall availability of the Space Station. Characteristic of integrated testing is the fact that the test involves subsystem interfaces, and, therefore, test objectives are associated with more than one subsystem.

4.2.1 INTEGRATED STRATEGY

Six checkout functions have been identified:

- Caution and warning
- Fault detection
- Trend analysis
- Operational status
- Periodic checkout
- Fault isolation

These functions represent a checkout strategy of continuous monitoring and periodic testing with eventual fault isolation to a line replaceable unit (LRU). Under this aspect the functions are grouped as -

CONTINUOUS MONITORING	PERIODIC TESTING	FAULT ISOLATION
• Caution and warning	• Automatic tests	• Localize to SS
• Fault detection	• Operational Verification	• Isolate to RLU
• Trend analysis		
• Operational status		

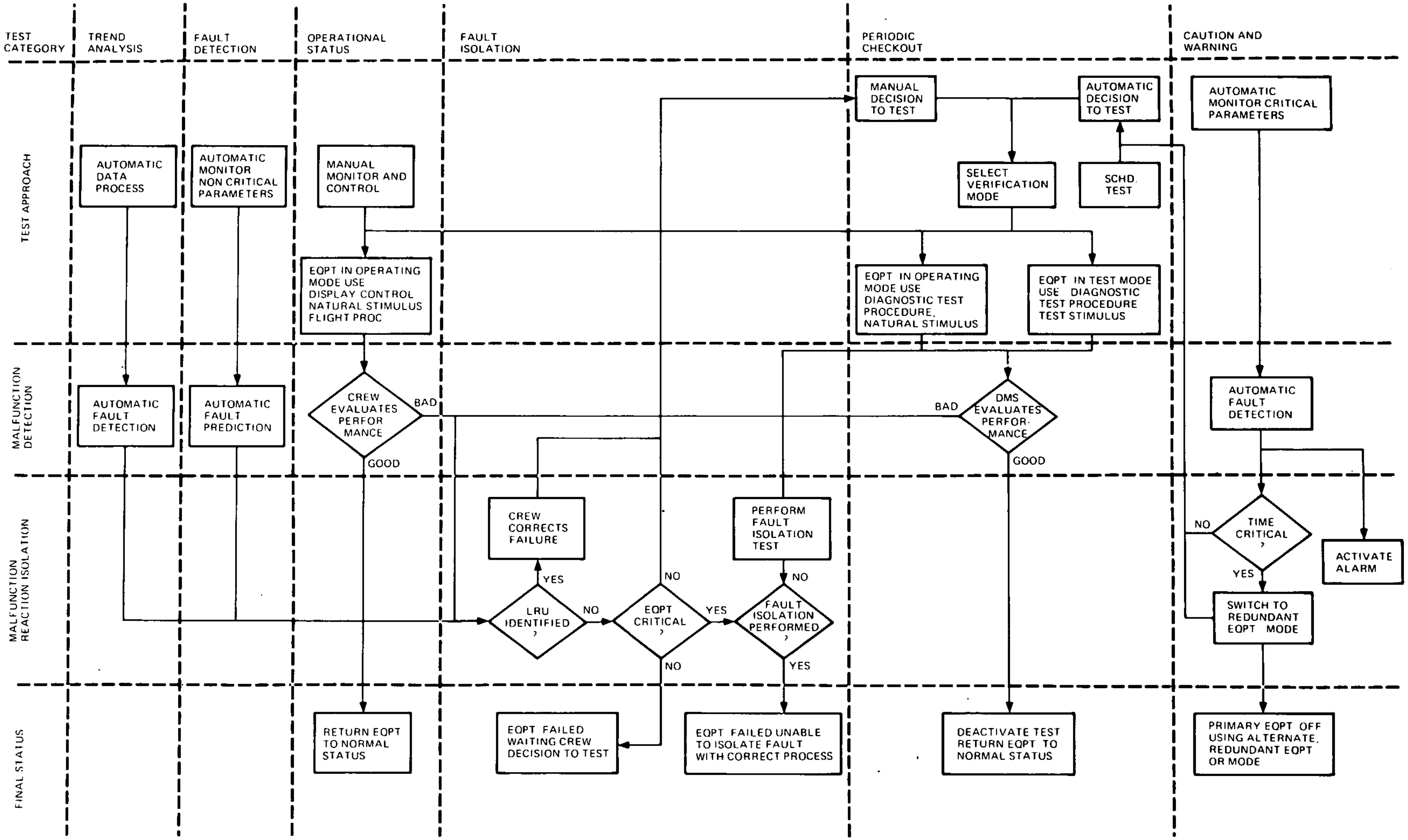


Figure 4-1. Integrated Checkout Functional Flow

General characteristics of these groups are defined below:

4.2.1.1 Continuous Monitoring

Continuous monitoring is not a test per se. It is a concept of continuously sampling and evaluating key subsystem parameters for in/out-of-tolerance conditions. This evaluation does not necessarily confirm that the subsystems have failed or are operating properly. The evaluation is only indicative of the general status of the subsystems. For example, a condition exists where the integrated subsystems are indicating in-limit conditions, but during the next series of attitude control commands, an error in Space Station position is sensed and displayed. Since three subsystems, DMS, GN&C, and P/RCS, are involved in generating and controlling the Space Station attitude, a "positional error" malfunction is not directly related to a subsystem malfunction. The malfunction indication is only indicative of an out-of-tolerance condition of an integrated function. Final resolution of the problem to a subsystem and eventually to LRU will require diagnostic test-procedures that are separate from the continuous monitoring function.

There are situations in which the parameters being monitored are intended to be directly indicative of the condition of a subsystem or an LRU. Examples of these include tank pressures, bearing temperatures, and power source voltages. However, even in these simpler cases when a malfunction is detected, an integrated evaluation will be performed to ascertain that external control functions, transducers, signal conditioning, and the DMS functions of data acquisition, transmission, and computation are performing properly. This evaluation will result in either a substantiation of the malfunction or identification of a problem external to the parameter being monitored.

Figure 4-1 shows the logic associated with each function in the continuous monitoring group, as well as the integrated relationships between these and the total checkout functions. The caution/warning and fault detection functions are alike in their automatic test and malfunction detection approaches, but are different in terms of parameter criticality and malfunction reaction. The caution/warning function monitors parameters that are indicative of conditions critical to crew or equipment safety. Parameters not meeting this criticality criteria are handled as fault detection functions. Figure 4-1 shows that in the event of a critical malfunction, automatic action is initiated to warn the crew and sequence the subsystems to a safe condition. Before this automatic action is taken, the subsystems must be evaluated to ascertain that the failure indication is not a false alarm and that the corrective action can be implemented. After the action is taken, the subsystems must be evaluated to determine that proper crew safety conditions exist. Since automatic failure detection and switching can be integral to subsystem design (self-contained correction) and subsystems can be controlled by the operational software or manual controls, it is imperative that the status of these events be maintained and that the fault detection and correction software be interfaced with the prime controlling software. For malfunctions that are not critical, the crew is notified of their occurrence, but any subsequent action is initiated manually.

The next continuous monitoring function, trend analysis, automatically acquires data and analyzes the historical pattern to determine signal drift and the need for unscheduled calibration. It also predicts faults and indicates the need for diagnostic and fault isolation activities. An example of a parameter in this category is the partial pressure of nitrogen. Nitrogen is used to establish the proper total pressure of the Space Station. Since it is an inert gas, the only make-up requirements are those demanded by leakage or airlock operation. The actual nitrogen flow rate is measured, and calculations are performed which make allowances for normal leakage and operational use. When these calculations indicate a trend toward more than anticipated use, the crew is automatically notified and testing is initiated to isolate the problem to the gas storage and control equipment or to an excessive leak path. The historical data is not only useful in predicting conditions but is also useful in providing trouble-shooting clues. The data might reveal, for example, that the makeup rate increased significantly after the use of an airlock. This could lead directly to verifying excessive seal leakage.

The final continuous monitor function is in operational status. This function is performed by the crew and is nonautomatic with the exception of the DMS computer programs associated with normal Space Station operational control and display functions. The concept of continuous monitoring recognized and takes advantage of the crew's presence and judgment in evaluating Space Station performance. In many instances the crew can discern between acceptable and unacceptable performance, and they can clearly recognize physically-damaged equipment or abnormal conditions.

4.2.1.2 Periodic Testing

As opposed to continuous monitoring, periodic testing is a detailed evaluation of how well the Space Station subsystems are performing. Figure 4-1 shows that periodic testing is not accomplished by any one technique. Rather, a combination of operational and automatic test approaches is employed. The actual operational use of equipment is often the best check of the performance of that equipment. Operation of Space Station equipment and use of the normal operating controls and displays will be used in detecting faults and degradation in the subsystems. This mode of testing is primarily limited to that equipment whose performance characteristics are easily discernible, such as for motors, lighting circuits, and alarm functions.

Automatic testing is performed in two basic modes:

- With the subsystems in an operating mode, the DMS executes a diagnostic test procedure which verifies that integrated Space Station functions

are being properly performed under normal interface conditions in response to natural or designed stimulation. This mode of testing allows the evaluation of Space Station performance without interrupting mission operations.

- For those situations where the integrated performance or interface compatibility between subsystems cannot be determined without known references or control conditions, the DMS will execute a diagnostic procedure in a test mode. In this mode, control, reference, or bias signals will be switched in or superimposed on the subsystems to allow an exact determination of their performance or localization of problem between the interfaces. Since the test mode may temporarily inhibit normal operations, the DMS must interleave the test and operational software to maintain the Space Station in a known and safe configuration.

The scheduled automatic tests are performed to verify availability or proper configuration of "on-line" subsystems, redundant equipment, and alternate modes.

- Periodic Verification of "On-Line" Subsystems - The first checkout requirement is a periodic verification that on-line subsystems are operating within acceptable performance margins. The acceptable criteria for this evaluation is based on subsystem parameter limits and characteristics exhibited during Space Station factory acceptance or pre-flight testing. The rejection criteria and subsequent decision to repair or reconfigure subsystems is based on the criticality of the failure mode. If the subsystems appear to be operating properly, but the test clearly indicates an out-of-tolerance condition, then one of the following alternatives must be implemented:

    - If the failure mode is critical, the crew normally takes immediate action to isolate and clear the problem.

    - If the failure mode is not critical, the crew can take immediate action, schedule the work at a later time, or wait until the condition degrades to an unacceptable level.

- Redundant Equipment Verification - A second checkout requirement is verifying that standby, off-line, or redundant equipment and associated control and switching mechanisms are operable. The acceptable/rejection criteria for these evaluations is identical to those for normally operating equipment. A primary distinction of this function is that equipment may have known failures from previous usage or tests. This situation occurs when the crew has knowledge of a failure but has not elected to perform the necessary corrective action. The checkout

function then becomes one of equipment status accounting and maintenance/repair scheduling. The status information is interlocked with mission procedures and software to preclude activation of failed units while they are being repaired or until proper operation following repair is verified.

- Alternate Mode Verification - The third checkout function is verifying the availability of alternate modes of operation. This function is essentially a confidence check of the compatibility of subsystems' interaction and performance during and after a change in the operating mode. To some extent this function overlaps with redundant equipment verification, but is broader in scope in that it verifies other system-operating characteristics. For example, some modes will involve manual override or control of automatic functions or automatic power-down sequences.

4.2.1.3 Fault Isolation

Fault isolation to an LRU is a Space Station goal. As shown in Figure 4-1, fault isolation testing is initiated when malfunction indications cannot be directly related to a failed LRU. The integrated test functions associated with fault isolation are localizing a malfunction to a subsystem or to an explicit interface between two subsystems and identifying the subroutine test necessary for LRU isolation. In structuring this relationship between integrated subsystem tests for fault localization and subroutine tests for fault isolation, the DMS, in conjunction with the test procedure documentation, must establish an effective man-machine interface so that in the event of an unsolved malfunction the crew will be able to help evaluate the condition and determine other test sequences necessary to isolate the problem. To accomplish this requirement, the DMS must be capable of displaying test parameters and instructions in engineering units and language and be capable of referencing these outputs to applicable documentation or programs that correlate test results to corrective action required by the crew.

Section 5

ONBOARD CHECKOUT TEST DEFINITIONS

5.1 SUBSYSTEM TEST DEFINITIONS

5.1.1 GENERAL CONSIDERATIONS

The on-orbit tests required to insure the availability of the Space Station subsystems are defined herein. Also delineated are the measurement and stimulus parameters required to perform these tests. Two discrete levels of testing are defined, i.e., continuous status monitoring tests for fault detection of critical and noncritical parameters, and subsystem fault isolation tests for localization of faults to a specific Line Replaceable Unit. In addition to these two levels, tests are defined for periodic checkout and calibration of certain units, and parameters requiring analysis of trends are defined.

Due to the software module approach to DMS checkout, it was deemed necessary to estimate the CPU time and memory required to implement these modules along with an assessment of the services required from an Executive Software System to control the checkout.

These test descriptions, measurement, and stimulus information provided for each subsystem, and the software sizing information provided for the Data Management System provide the data required to estimate the checkout impact on the DMS software and hardware. Table 5-1 is a summary of the measurement and stimulus requirements for the Space Station.

The Propulsion Subsystem consists of two major elements, one being the High-Thrust Monopropellant Hydrazine System and the other the Low-Thrust Resistojet Thruster System. Both systems interface with the GN&C and Data Management Subsystems for control. The Low-Thrust System also interfaces with the EC/LS Subsystem for biowaste propellants.

5.1.1.1 High-Thrust Propulsion Subsystem

The High-Thrust Propulsion System must satisfy both an initial Space Station two-year artificial-gravity phase and subsequent zero-gravity phase. The quantity of subsystem measurements and stimuli required for the former are more than double the quantity required for the latter. This is due to increased propellant and pressurant tankage requirements as well as the increased number of thrusters necessary during artificial gravity operations.

Operation of the High-Thrust System is automatic with the thruster firing controlled by the GN&C Subsystem. All other normal operational controls for the subsystem are associated with tank switching, thermal control, and safing functions. The need for tank switching is monitored and controlled by the DMS, while the thermal control assemblies are controlled by various thermostats.

Table 5-1. Measurement/Stimulus Summary

SUBSYSTEM	STIMULUS Analog	STIMULUS Bilevel	STIMULUS Digital	STIMULUS Pulse	STIMULUS RF	RESPONSE Analog	RESPONSE Bilevel	RESPONSE Digital	STATUS MONITORING Total	STATUS MONITORING Non-Critical	STATUS MONITORING Caution	STATUS MONITORING Warning	Periodic Checkout	Cali-bration	Trend	Fault Isola-tion	Remarks
Guidance, Navigation and Control	20	146	62	6		127	161	70	592	130	16		516	74	74	592	
Propulsion - Low Thrust		134				120	124		378	152	14		378	48	8	378	
Propulsion - High Thrust		126/62				287/117	123/63		536/242	80/28	33/15	14/10	536/242	259/111	117/43	482/222	Art-g/Zero-g periods
Environmental Control/ Life Support	34	111				691	280		1116	139	205	32	1116		135	1116	172 Caution/Warning Signals are for IVA/EVA
RF Communications	37	206	36		77	131	286	28	801	58			576	24	93	801	
Structures	15/16	21/19				60/53	75/66		174/154	7			123/104			174/154	
Electrical Power - TCD	52	1952				292	1292	20(1)	7608	1404	20		724		134	3608	(1) Twelve of these take pulse form
Electrical Power - Solar Array/Battery		1916				4044	928		6780	3704	12		2184		332	6788	
Data Management			53			33	188	83	357	357			62	62	62	357	
Total	151/169	4512/ 4446	151	6	77	5785/ 5628	3457/ 3388	201	14,350/ 14,035	6031/ 5979	300/282	46/42	5110/ 5902	467/ 319	935/ 861	14,266/ 14,016	

Although the High-Thrust System is normally required only during scheduled events such as the artificial-gravity experiment or docking, the system is continuously maintained in a pressurized and ready-to-fire state. This concept is strongly influenced by fluid characteristics, resupplying penalties, and the need for the subsystem to be available for unscheduled events or emergencies. Safety parameters as well as certain other system status and readiness indicators are therefore monitored continuously even though the system may be inactive. Scheduled high-thrust events are typically at three-month intervals and are critical in nature. A complete functional check of the system is therefore required prior to each event. Resupply operations are also scheduled every three months and require that leak and functional checks of the transfer system lines and controls be performed. During the events and particularly during actual thruster firing intervals, subsystem status monitoring requirements become extremely important. Appendix I-2 of the Task 1 Final Report contains the measurements and stimuli required for checkout of the High-Thrust Propulsion Subsystem.

5.1.1.2 Low-Thrust Propulsion System

The Low-Thrust Propulsion System uses EC/LS-produced biowaste gases (CO_2, H_2O, CH_4) and stored water as propellant for resistojet thrusters. These thrusters have a thrust level of 25 millipounds, and are used in a high duty cycle mode (25-80 percent) to provide station orbit maintenance and, if desired, CMG desaturation. The system consists of compression pumps, heat exchangers, accumulators, supplementary propellant tankage, thrusters, and the necessary valves, switches, etc., for system control, checkout, etc.

Normal system operation is in the orbit-keeping and attitude control mode and is fully automatic. Thruster selection and control is derived by the DMS computational equipment on the basis of inputs from the GN&C Subsystem. The DMS also controls the subsystem configuration parameters such as propellant and pressurant selection. These parameters are primarily a function of impulse requirements and available stores. Manual control capability is provided to allow crew override if required due to a malfunction or other reasons. On-orbit checkout of the low-thrust system includes a combination of continuous monitoring, daily operational status checks and trend analysis, a detailed periodic checkout every three months, and fault isolation activities. Appendix I-3 of the Task 1 Final Report contains the measurements and stimuli required to check out the Low-Thrust Propulsion System.

5.1.2 STATUS MONITORING

5.1.2.1 High-Thrust Propulsion Subsystem

Continuous monitoring of high-thrust propulsion system parameters is performed to detect over-pressure conditions, out-of-tolerance regulation, major leakage, empty tankage, and thruster malfunctions:

- Overpressure - Each tank is relieved automatically through a burst disk and mechanical relief valve when a major overpressure condition arises. Tank pressure as well as relief valve actuation is monitored continuously with a signal initiated to alert the crew of any unwarranted pressure build-up.

- Out-of-Tolerance Regulation - Redundant pressure regulation is provided by parallel regulators, and automatic malfunction detection and switching is provided by pressure switches which activate the valves to each regulator. Pressure switches initiate the appropriate commands dependent on the malfunction mode (high or low regulation outlet pressure). A signal is also provided to alert the crew to any regulator switchover.

- Major Leakage - Pressure transducer signals are monitored continuously, and pressure decay rates are computed. An indication of any abnormal pressure decay requires the initiation of closing the appropriate isolation valves.

- Tank Switching/Isolation - Any pressure differential across the propellant tanks (gas ullage to fluid side) is detected and the appropriate switching commands initiated. This differential pressure occurs when a tank runs dry thus requiring the next tank (normally isolated) to be put on-line to feed propellant to the thrusters.

- Thruster Out-of-Limit Operating Pressure, Temperature, and Voltage Conditions - The thruster, to operate safely, must have specific inlet conditions. These conditions are monitored and thruster operations inhibited if they are out of limits.

5.1.2.2 Low-Thrust Propulsion Subsystem

Continuous monitoring of low thrust system parameters is conducted to detect faults and to initiate switching to redundant LRUs when necessary. This is accomplished by a combination of integral sensing/switching provisions and DMS action. The integral implementation is utilized primarily in the case of failures which demand immediate and direct action to relieve a potentially hazardous condition. An example is excessive pressure on the outlet side of a pressure regulator. The condition would be detected by a pressure sensitive switch which, when activated, would automatically operate solenoid valves to isolate the regulator and switch to a parallel redundant unit. Notification of the occurrence would be given the DMS which would then proceed to notify the crew and accomplish other required reactions, such as fault verification, repair direction, or modification of Space Station operations. Faults which are less critical in nature and those for which diagnosis and corrective action require the computational and analytical capability of the DMS are processed by automated DMS routines. Table 5-2 lists a number of representative failure modes and the associated subsystem or DMS action.

5.1.3 TREND ANALYSIS

Trend analysis is utilized for functions which are subject to performance degradation of known and measurable characteristics. By observing the change in the major performance parameters, component replacement can be scheduled at a convenient time for the crew. Hazardous conditions can be avoided by trend analysis prediction of out-of-tolerance conditions. Trend analysis is also used to monitor expendable use rates. This pin-points locations of excessive expendables use rates indicative of possible leakage or other failures, and also provides a basis for resources management and resupply planning activities.

Table 5-2. Representative Failure Modes and Associated Subsystem or DMS Action

COMPONENT	FAULT	ACTION
Pump	Excessively high or low pump speed	DMS turn off pump and isolate by closing appropriate valves.
Pump	Out-of-limit inter-stage temperature	Same as above, initiated by measurement in EC/LS Subsystem.
Storage bottle and/or High Pressure Manifold	Excessive pressure	Relief assembly vents gas(es). Integral control.
Regulator	Out-of-tolerance regulation	Switch to alternate regulator and isolate by closing appropriate valves. Integral control.
Flow Control Valve	Fail close or open	DMS switch to alternate feed system and isloate by closing crossfeed valves.
Thruster	Heating element over temperature	Integral thruster cutoff.
Thruster	Out-of-tolerance power consumption	DMS switch to alternate thrusters.
Thruster	Inlet valve will not close	DMS switch to alternate thruster and isolate module.
Fittings	Leakage	DMS or crew inspection determine source and isolate. Switch to alternate assembly.
H_20 Vaporizer	Out-of-tolerance heat input	DMS switch to alternate vaporizer. Turn off heaters and close isolation valves.
H_20 Storage	Out-of-tolerance pressure	DMS-switch to alternate tank and isolate.

5.1.4 PERIODIC CHECKOUT AND CALIBRATION

5.1.4.1 High Thrust

Daily checks of the High-Thrust System are conducted to determine its operational status. A more detailed verification is also performed approximately every three months.

Typical daily subsystem status checks are accomplished through visual monitoring of displays and through automatic limit checks and trend analysis. The following status checks are required:

- Subsystem Status - Insures that the subsystem is in an operational state (satisfactory pressures, temperatures, valve positions, propellant, and pressurant quantities, etc.).

- Primary or Backup Assembly Status - Provides an indication of whether the redundant or primary subsystem assemblies are in use.

- Tank Pressures and Temperatures - Verifies that normal operating conditions exist and whether pressure and temperature variation trends are normal.

The more detailed periodic checkout is scheduled over three-month intervals and prior to initiation of a critical operation such as an artificial experiment.

In cases where a fault is detected, the applicable portions of the periodic checkout procedure will be needed to determine the maintenance required. The periodic checkout includes:

- Leak and Functional Tests - These verify the basic subsystem integrity. Leak tests are performed both manually and automatically. The manual checks are required to detect low-rate leak conditions which may be detrimental over a long period of time if uncorrected. The functional tests check both the electrical circuits and component (valves, etc.) operations.

- Pressure Regulation and Thruster Performance Checks - The thruster performance checks require monitoring and recording of chamber pressure and temperature versus time during the firing interval. Automatic/programmed test-sequencing and high-speed data sampling at a rate of 250 samples/second are necessary.

- Instrumentation Calibration - One or two-point calibration is required for both temperature and pressure transducers. Use of standard gages or known pressure and temperature references is required.

- GN&C/Propulsion Subsystem Interface Checks - Simulated programmed control commands are needed to verify the GN&C propulsion interfaces. Other subsystem (DMS and Electrical Power) interface integrity checks are also performed as part of the periodic functional tests.

- Propellant Sampling - The quality of the propellant must be determined through taking a sample and returning it on the ALS for analysis on the ground.

- Subsystem Hardware Life History Log - Automatic storage and display of data is desirable.

In general, the test sequence for the detailed periodic checkout should first include an evaluation of general subsystem status and safety critical parameters followed by LRU-level checkout. The general test sequence should be to test the high pressure storage assemblies first and then the subsequent downstream assemblies. A total candidate sequence follows:

(a) Subsystem Status Check

- Pressure
- Temperature
- Valve Position
- Propellant Quantity
- Identification of On-Line Equipment

(b) Pressure Transducer Calibration Check

(c) Verify Purge (Checkout) Assembly Operational Status

- Functional
- Pressure (Regulation)

(d) Subsystem Gross Leakage Test

- Pressure Trend/Analysis

(e) Verify Safety Critical Caution and Warning Circuits (over pressure, relief actuation, regulator switchover, etc.)

- Electrical Continuity/Response

(f) Bellows Leak Test

- Gas Analysis of Pressurant

(g) Pressure Control Assembly Check

- Backup Regulator Switchover Circuit
- Regulation
- Pressure Switch Setting

(h) High Pressure Isolation Valve Check

- Leakage - Pressure Trend Analysis
- Functional

(i) Test Low Pressure Manifold and Propellant Tank (Gas Side) Isolation Valves

- Leakage - Pressure Trend Analysis
- Functional

(j) Test Propellant Isolation Valves (Tanks and Manifolds)

- Leakage - Pressure Trend Analysis
- Functional

(k) Check Tank Switching Circuit

- Functional

(l) Thruster Modules

- Isolation Valves - Leaks and Functional
- Isolation Circuits
- Thruster Valves - Leakage
- Thruster - Functional and Performance Firing

(m) Miscellaneous

- Vent Valves - Leak and Functional
- Catalytic Nonpropulsive (propellant) Vent Device - Functional
- Temperature Sensors - Calibration
- Resupply Subassembly

(n) GN&C - Propulsion Integrated Subsystem Test

- Functional - Firing Commands
- Performance - Chamber Pressure and Temperature versus Time Verification

5.1.4.2 Periodic Checkout and Calibration - Low Thrust

As for the High-Thrust System, daily operational status checks are required for the Low-Thrust System. These daily checks are basically the same as those described in Subsection 5.1.4.1.

A more detailed checkout of the Low-Thrust System is conducted every three months. All redundant elements within the system are checked, including a verification of the proper operation of all valves. The daily checks only verify valve positions, not valve actuation. A possible test sequence to be used in the periodic checkout is:

- Subsystem Status Check
  - Pressure
  - Temperature
  - Valve Position

- Propellant Quantity
- Identification of On-Line Equipment
- Pump Speed
- Vaporizer

- Pressure Transducer Calibration Check (only every 6 months)
- Subsystem Gross Leakage Test
  - Pressure Trend Analysis
- Verify Safety Critical Caution Circuits (over pressure, relief actuation, regulator switch-over, etc.)
  - Electrical Continuity/Response
- Flow Control Check
  - Backup Regulator Switchover Circuit
  - Regulation
  - Pressure Switch Setting
  - Valves
- Thruster Modules
  - Isolation Valves - leaks and functional
  - Isolation Circuits
  - Thruster Valves - leakage
  - Thruster Heaters
- Interface Checks
  - GN&C
  - EC/LS

5.1.5 FAULT ISOLATION

5.1.5.1 High-Thrust Propulsion Subsystem

Fault isolation checks within the High-Thrust Propulsion Subsystem consist essentially of portions of the detailed periodic checkout sequence previously described. An example of isolating a fault following the detection of a change in the regulator isolation valve is depicted in Figure 5-2. The following steps are required to isolate a fault in the pressure control assembly. The example is considered to be one of the more complex fault isolation tests for the high thrust system.

1. Verify subsystem operational status.
2. Calibrate hi pressure and pressurant manifold pressure transducers.
3. Verify purge (checkout) assembly is operational.
4. Close propellant tank pressurant isolation valves, low pressure manifold isolation valves, and regulator isolation valves.
5. Verify regulation isolation valves are functional.
6. Vent low pressure manifold.
7. Open primary regulator isolation valves.
8. Monitor downstream regulation pressure - either a high or low regulation pressure failure indication should occur. If the regulator proves to be satisfactory, the pressure switches or switchover circuits are malfunctioning.
9. Close regulator isolation valve and provide pressure switch test pressures from the purge (checkout) assembly. Verify pressure-switch actuation pressure valves. If the pressure switch performance is satisfactory, the control logic circuits must be malfunctioning.
10. Conduct electrical switchout circuit repair and checks as required. (Note: The Electrical LRUs have not been identified for the Propulsion Subsystem.).
11. Reset regulator switchover circuit and assure the pressure control assembly is in an operational state.

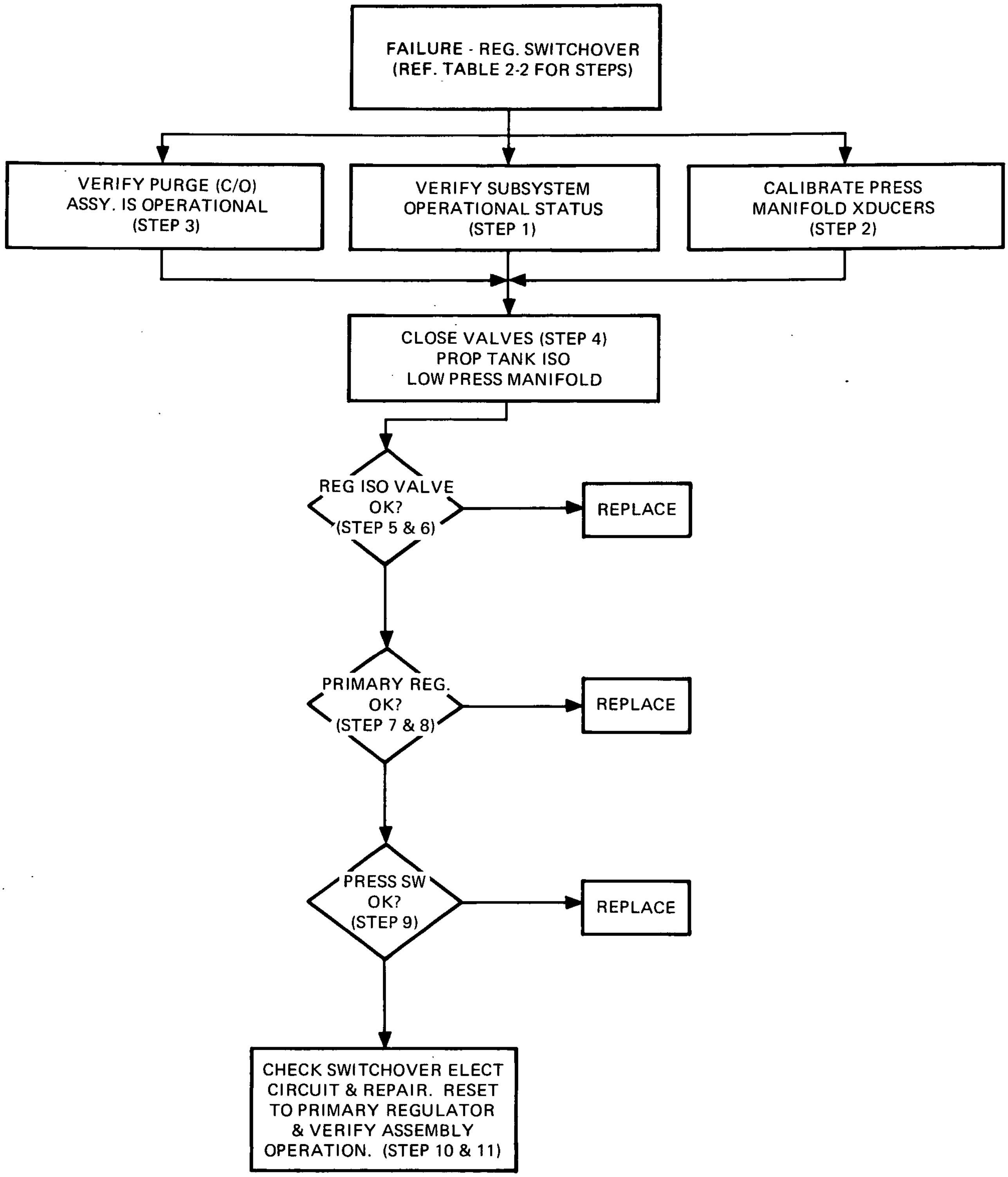


Figure 5-2. Fault Isolation Check Pressure Control Assembly

5.1.5.2 Low-Thrust Propulsion Subsystem

Fault isolation within the Low-Thrust System typically involves an input/output relationship such as regulator inlet versus outlet pressure, valve command versus position, etc. A typical fault isolation flow is depicted in Figure 6-3 for a CO_2 tank isolation valve failure. The failure is detected as a result of monitoring valve position, and the crew is notified of switchover to the redundant valve. For this case, the failure is either the valve or in the DMS control logic or data acquisition elements.

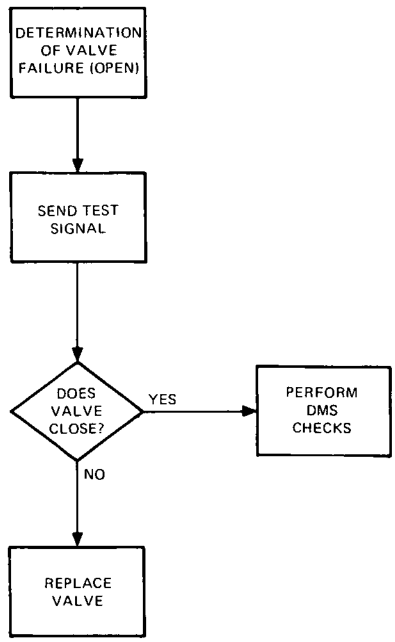


Figure 5-3. Low Thrust System CO_2 Tank Isolation Valve Failure (Open)

The capability to substitute redundant elements provides a very useful fault isolation tool for the Low-Thrust System. This may be used in the case of the pressure regulator assemblies, compression pumps, and water vaporizers for example, where solenoid-controlled isolation and cross feed valves allow rapid switchover to the redundant elements.

5.2 INTEGRATED TEST DEFINITION

The task of ensuring overall Space Station availability is primarily dependent upon the proper structuring of individual subsystem tests. The ability to test the subsystems independent of other subsystems is directly related to the number and types of interfaces. As shown in Figure 5-4, the DMS and Electrical Power Subsystems (EPS) interface with every other Space Station subsystem. In addition, the EC/LS Subsystem provides cooling to most of the electronic packages.

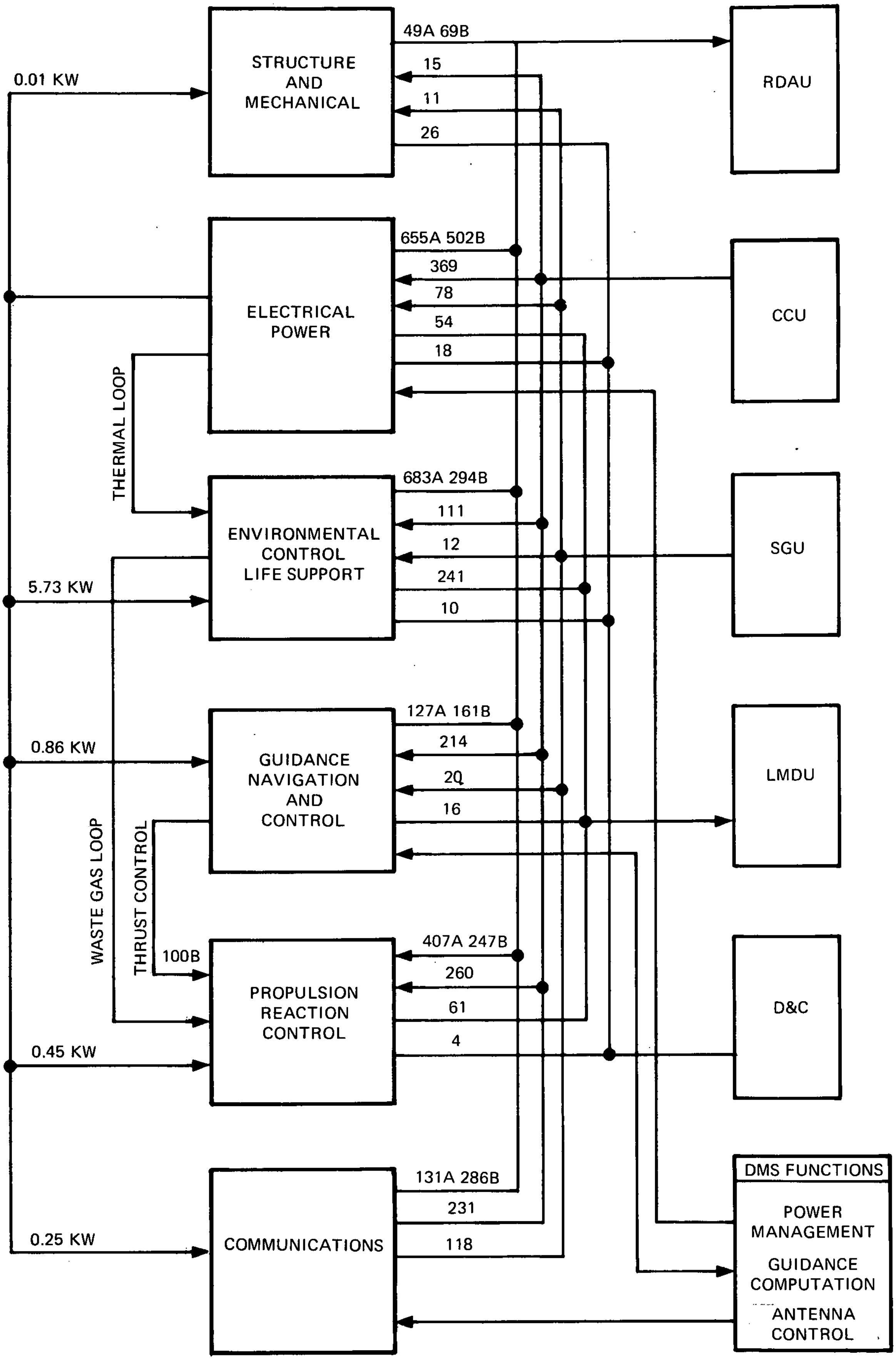


Figure 5-4. Subsystem Interfaces

This situation demands that in constructing the test for a subsystem these interfaces be taken into account so that erroneous or ambiguous test results will not be obtained. In other words, before detailed subsystem fault isolation tests are initiated, a higher level of testing should be performed to verify that all interfaces and Space Station conditions that influence the subsystem are proper. Properly designed, these higher-level tests will (1) indicate what Space Station conditions must be verified, maintained, or changed; (2) localize the malfunction to a single subsystem; and (3) identify the subroutine test necessary for fault isolation.

Since the DMS interfaces with all of the Space Station subsystems and is used as the OCS, it would appear that all of the tests would be integrated. However, this is not a proper interpretation. When the DMS is used to verify the performance of another subsystem, it must first establish itself as a test standard against which the subsystem parameters are compared. Subsequent to this verification, the test is dedicated to the evaluation of the subsystem. This test would be considered as an independent test since the objective of the test was to verify the subsystem and not the DMS. For a test to be considered as an integrated test it must meet one or more of the following conditions:

- Test objectives associated with more than one subsystem
- Test involves subsystem interfaces
- Test requires proper operation of other subsystems

In several cases, the DMS must simultaneously perform the dual role of OCS and functional elements. As an example, the DMS has a functional interface with the GN&C and Prop Subsystems for the computation of guidance equations and the execution of commands to the control actuators. When this functional closed loop is being tested, the DMS must, in addition to performing its normal functions, execute the test routine. For this type of integrated test there must be an intrinsic relationship between the operational and test software. This relationship must be carefully considered in structuring the integrated tests since unstable or intermittent performance may be detected only in the exact operating mode under closed-loop conditions. The number of integrated tests is not extensive due to the approach of minimizing the different types of interfaces between Space Station subsystems. For example, interfaces between the DMS and other subsystems are largely standardized. As a result, relatively common tests can be designed for verification of the multitude of DMS subsystem interfaces or for localization of a fault to one side of a DMS subsystem interface. All special integrated tests that have been identified are discussed in the following paragraphs. The GN&C/DMS/PROP configuration for navigation and attitude control poses the most difficult problem for on-orbit testing so it is presented in significant detail. Other integrated tests are summarized.

5.2.1 GN&C/DMS/PROP

5.2.1.1 Block Diagram

Figure 5-5 shows the block diagram for the GN&C/DMS/PROP Subsystems as configured for the zero g, horizontal mode of operation. The subsystems are shown at the LRU level with all primary functional interfaces. For simplicity, prime power inputs, cold plate interfaces, and mechanical or fluid connections are not shown.

5.2.1.2 Functional Description

The GN&C Subsystem accommodates both the artificial-g and zero-g operations of the Space Station. In the zero-g mode of operation, the GN&C Subsystem provides autonomous navigation, rendezvous command, traffic control, automatic docking, and stabilization and control of the Space Station.

The autonomous navigation scheme utilizes the stellar inertial reference data and the automatic landmark tracker augmented with the drag accelerometer. The navigation is accomplished by automatically tracking known and unknown landmarks several times each orbit. The landmark is similar in operation and mechanization to a gimballed star tracker. The drag accelerometer accounts for anomalies due to Space Station orientation and docked module changes which contribute to navigation errors.

Both ground tracking and onboard subsystems will provide the navigation information for the first year or so of the Space Station Program. The ground-generated data will be transmitted onboard for evaluation of the autonomous navigation system performance. As the confidence in autonomous operation is increased through this parallel operation, the ground tracking is to be phased out.

In all operating modes and orientations, the gyros provide the high-frequency rate and attitude information necessary to supplement the data from the stellar sensors and the horizon sensors.

A more accurate Earth-centered reference is obtained in the horizontal orientation through the use of the strapdown star sensors. The star sensors provide the long-term, drift-free inertial reference data while the gyros provide the short-term, high-frequency attitude and rate information. The passive star sensors are used while the Space Station is maintained in an Earth-centered orientation. The constant rotational rate required of the vehicle to maintain this type of orientation provides the scanning motion for the star sensors, which are completely passive and provide no tracking or scanning capability of their own.

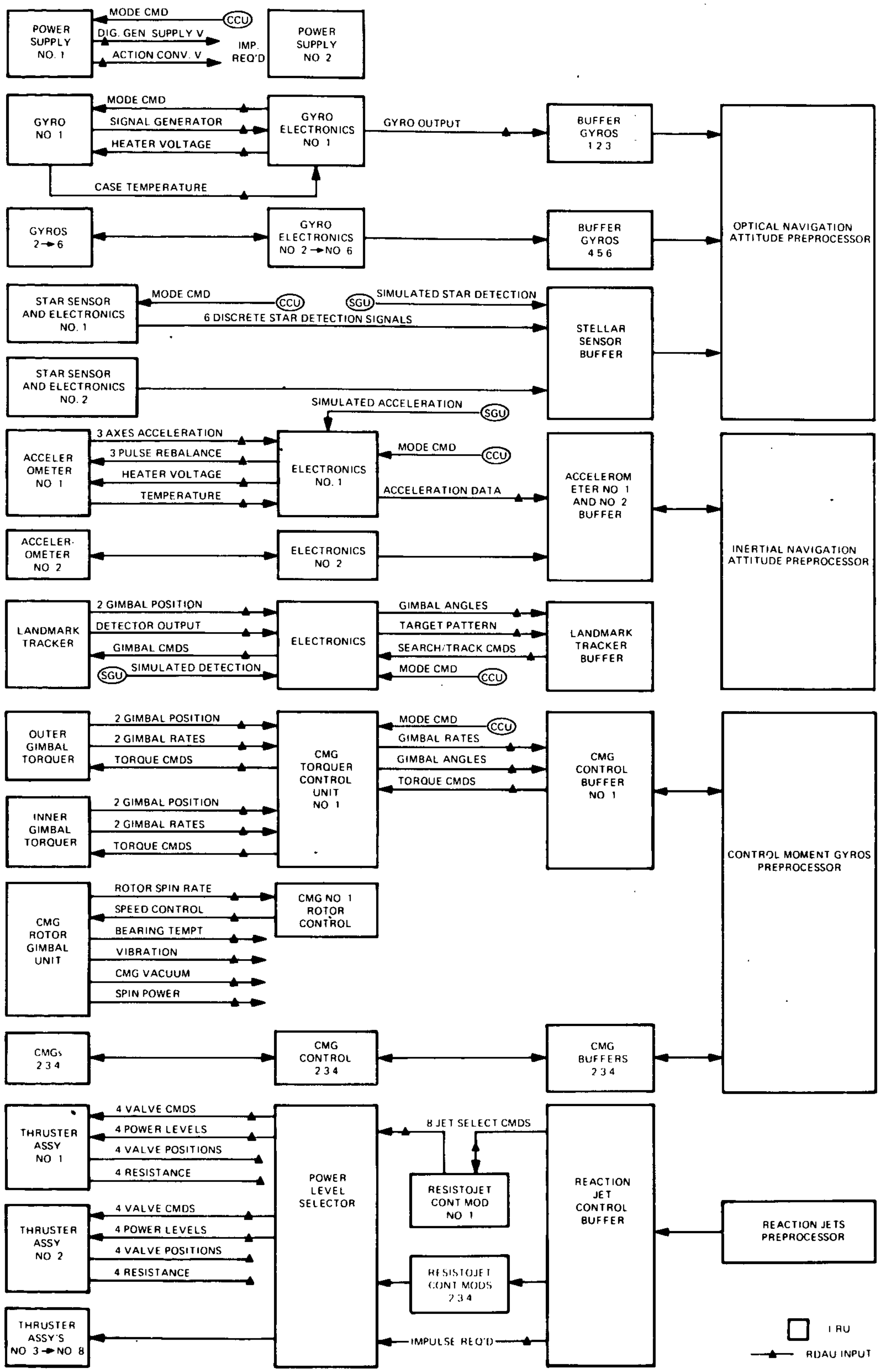


Figure 5-5. GN&C/DMS/PROP Configuration for Zero-G Horizontal Mode

The sensors themselves provide inertial attitude data which is transformed into Earth-centered attitude information by use of the navigation parameters. By this method, both inertial attitude and Earth-centered attitude are derived from the passive star sensors while the vehicle is in the horizontal or other Earth-centered orientation. This Earth-centered orientation is considered to be most responsive to experiment and subsystem requirements.

Primary attitude control actuation is provided by control moment gyros (CMGs). A CMG configuration utilizing four double-gimballed CMGs, each having a momentum capacity of 1,100 ft-lb-sec, was selected for the isotope/Brayton-powered Space Station. Both High and Low-Thrust Propulsion Systems are utilized by the GN&C Subsystem for CMG desaturation and backup attitude control capability. The reaction jet control buffer provides the interface with the Propulsion Subsystem.

The DMS provides the link between the sensors, which are used to determine the vehicle angular position, and the actuators, which are used to maintain or change the vehicle angular position. The use of the DMS provides the flexibility required during both the development and operational phases to accommodate the total Space Station Program objectives. The DMS performs the data processing necessary for all guidance, navigation, and attitude control functions. The interface electronics controls the flow of information from the sensors to the DMS and converts all sensor inputs to a standardized format before the inputs are transferred. The interface electronics performs a similar function for output information from the DMS to the control actuators.

5.2.1.3 Test Flow

The test flow for the GN&C/DMS/PROP configuration is shown in Figure 5-6. The flow demonstrates the technique for malfunction detection, subsystem localization and fault isolation to the LRU. For simplicity some tests associated with prime power, mode commands and cold plate temperatures are omitted. It is assumed that in programming the actual tests these types of measurements will be implemented as standard procedure. In the same vein, detailed tests of the DMS are not shown. Again, it is assumed that the final procedure would contain the necessary self-test, command verification, and other checks to maintain confidence in DMS performance throughout the test.

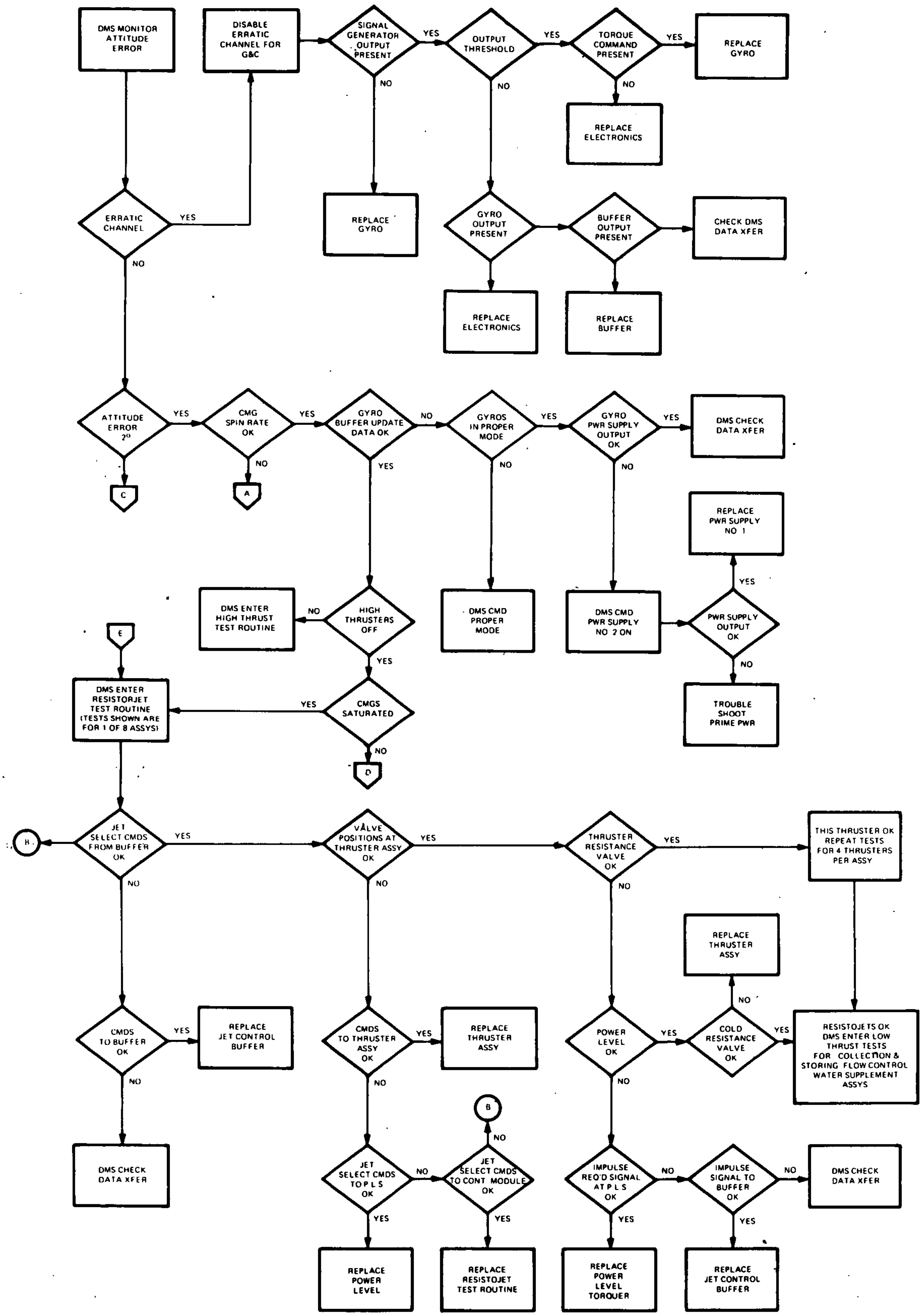


Figure 5-6. GN&C/DMS/PROP Integrated Test Flow (Sheet 1 of 4)

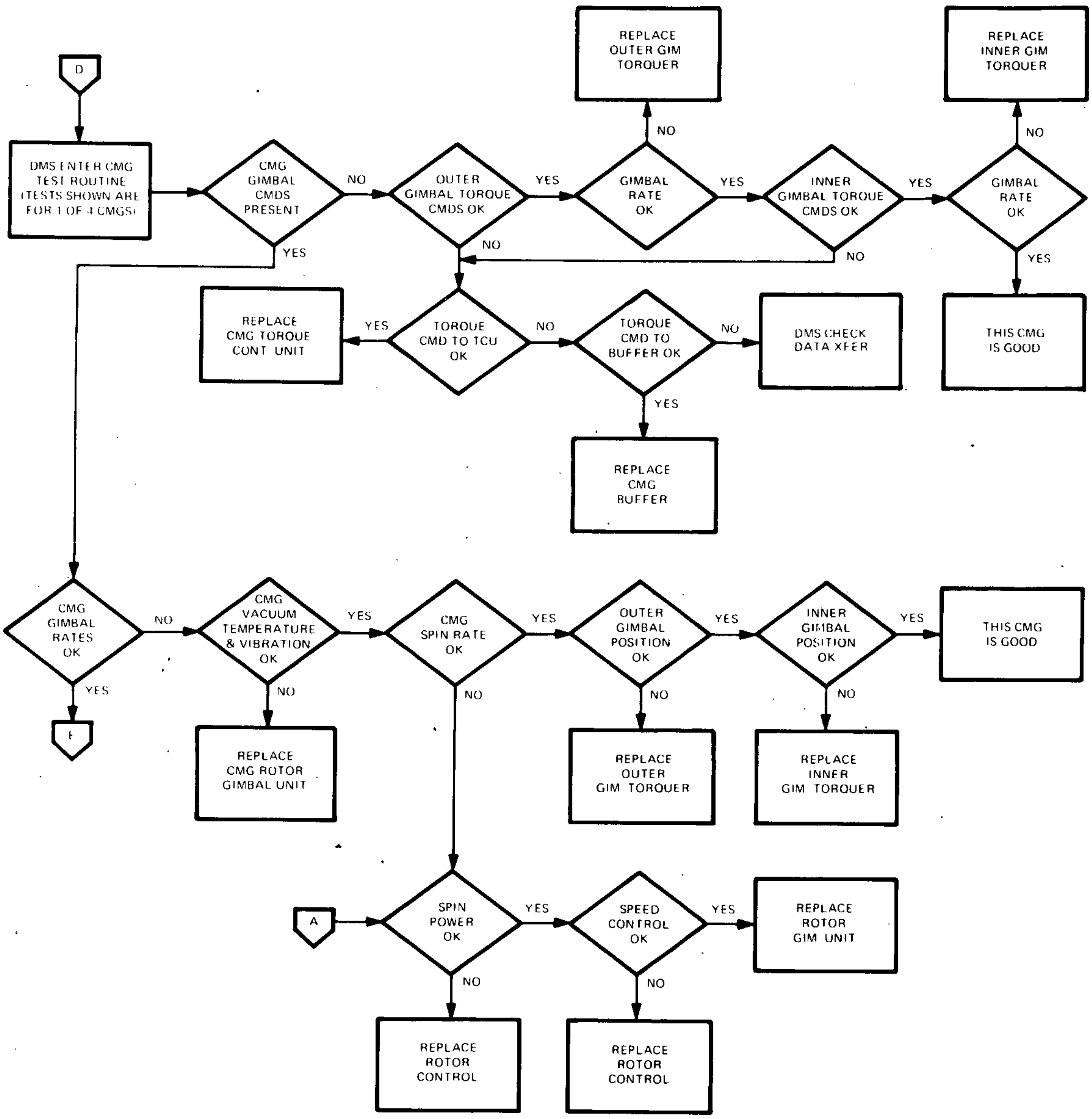


Figure 5-6. GN&C/DMS/PROP Integrated Test Flow (Sheet 2 of 4)

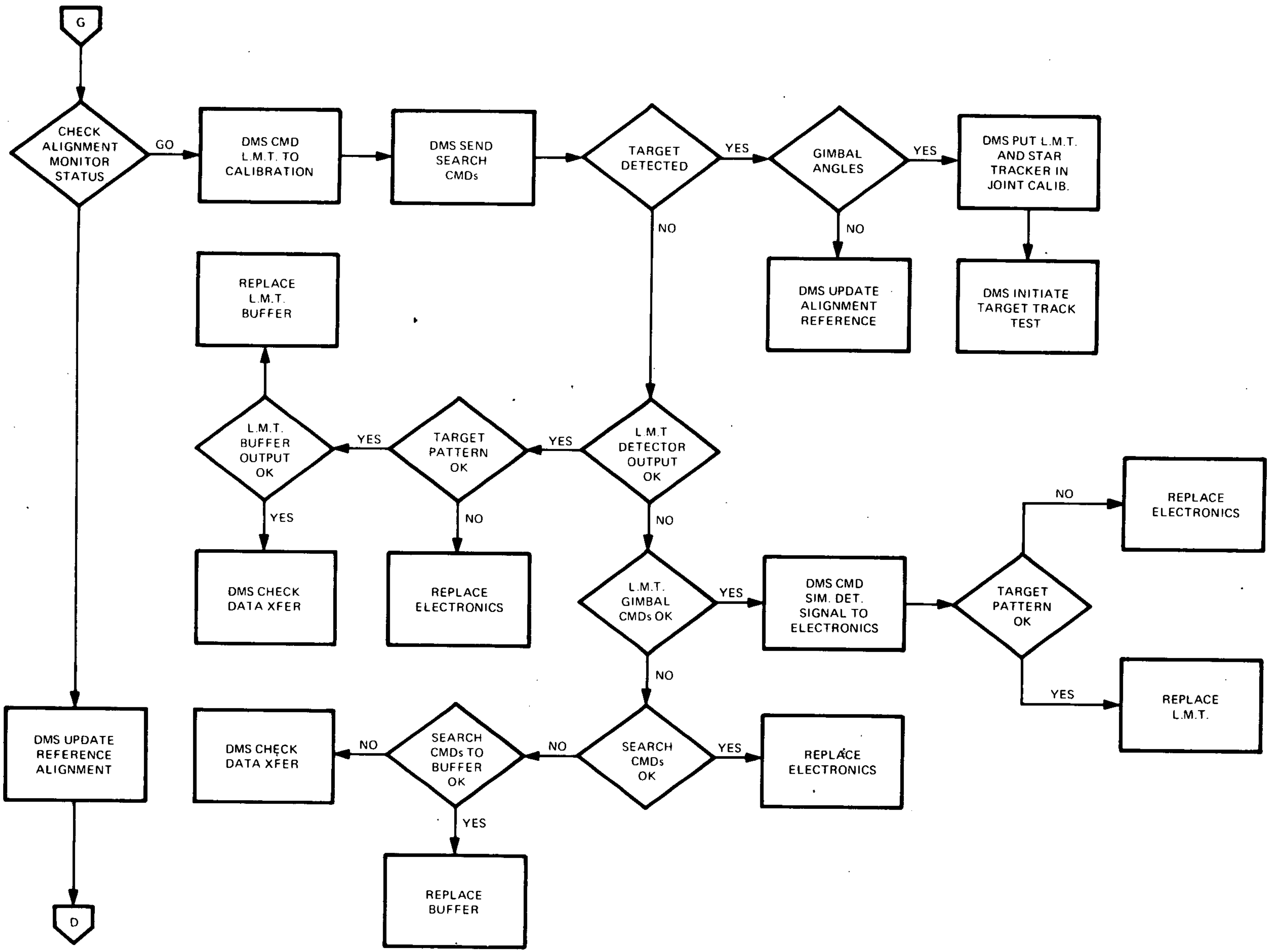


Figure 5-6. GN&C/DMS/PROP Integrated Test Flow (Sheet 3 of 4)

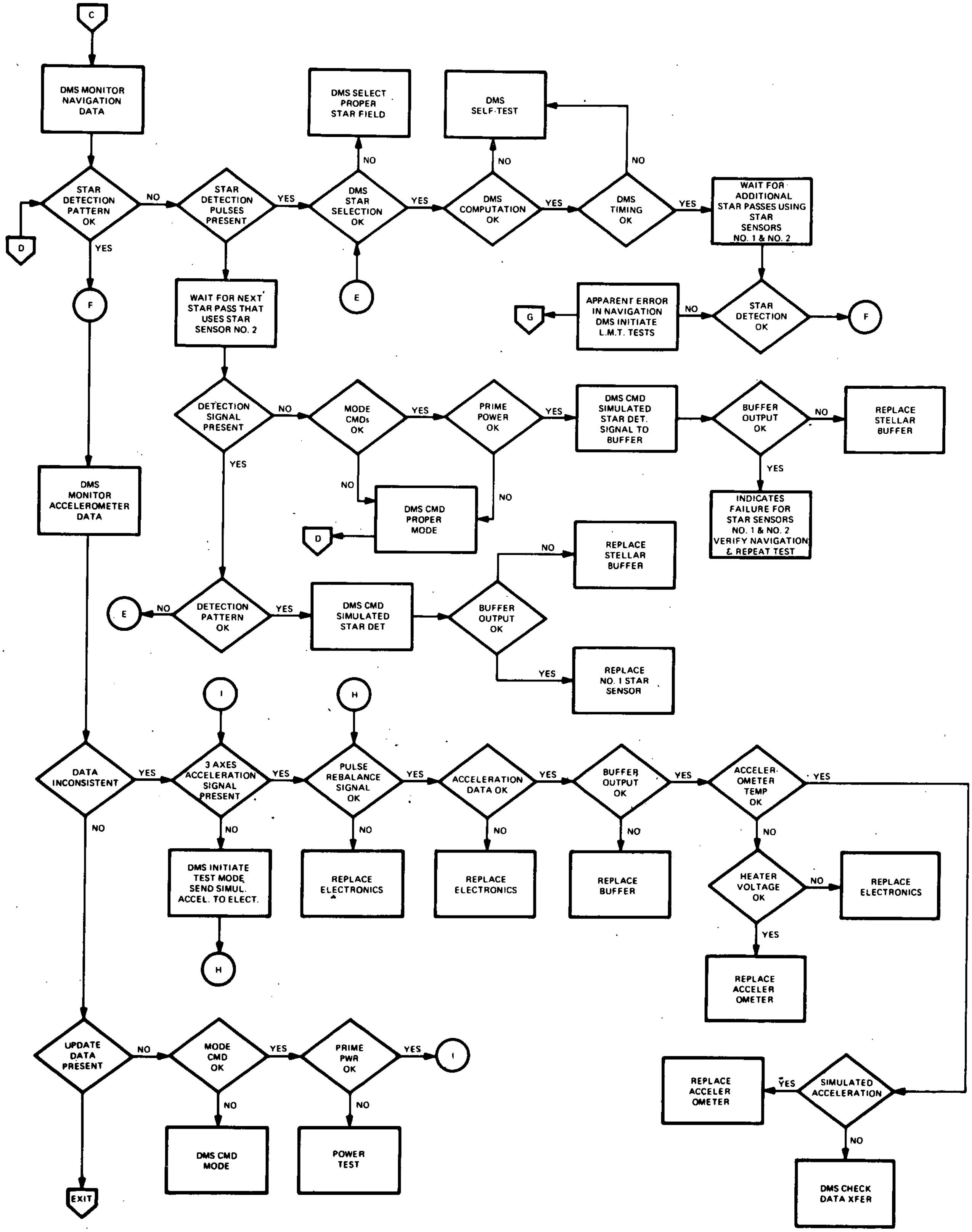


Figure 5-6. GN&C/DMS/PROP Integrated Test Flow (Sheet 4 of 4)

Many of these test sequences will be repeated for different channels of data or for identical sets of equipment. The test flow does not show the repetition of these tests but indicates the need for them. For example, there are four control moment gyros (CMGs). The flow shows a typical test for one CMG. It should be pointed out that although the detail test sequence will be identical for all CMGs, the absolute value of the parameters such as torque commands, gimbal position, gimbal, rates will be different for all CMGs. In some cases, the test flow terminates in an instruction for the DMS to check data transfer. This instruction is intended to include all operations necessary to verify that the DMS is functioning as required to support the operational and test routine.

5.2.2 GN&C/DMS/COMM

The DMS has a functional interface with the GN&C and COMM Subsystems for the pointing and control of antennas. The GN&C sends navigation and attitude information to the DMS which in turn uses it to compute antenna pointing positions and slewing rates. Once computed, the DMS transfers these commands to the antenna actuators in the Communication Subsystem.

Localizing a malfunction to one of the three subsystems will be performed in a manner similar to that described in subsection 5.2.1. The DMS will verify receipt of proper attitude and navigation data from the GN&C Subsystem, check its capability to operate on and transform the data into appropriate antenna commands, and verify the transmission of the control data to the Communication Subsystem. Verification of proper response and operation of Communication Subsystem equipment will be aided by the switching and use of redundant transmitters and receivers.

5.2.3 GN&C - PROPULSION SUBSYSTEM INTERFACE

The Guidance, Navigation, and Control (GN&C) Subsystem operates in a closed-loop mode with the DMS and Propulsion Subsystem as elements of the loop. Electrical signals to activate appropriate Propulsion Subsystem high thrusters are provided by the GN&C jet drivers based upon control information computed by the DMS. Although the interface between the DMS and the GN&C is fairly complex, the GN&C - Propulsion Subsystem interface is not, and can easily be incorporated into tests defined for the Propulsion Subsystem.

Section 6

SOFTWARE

6.1 GENERAL CONSIDERATIONS

The recommended software checkout startegy involves a sequence of detecting faults, isolating faults to a failing LRU or LRUs, and reconfiguring the system to continue operation while the failures are being repaired.

This recommendation was developed by evaluating each subsystem with respect to the three general requirements of fault detection, fault isolation, and reconfiguration.

Fault detection incorporates both the recognition of failure occurrence, and the prediction of when a failure can be expected to occur. The Remote Data Acquisition Units (RDAUs) continually check selected test point measurements against upper and lower limits, and notify the executive on an exception basis when a limit is exceeded. This approach avoids occupying the central multi-processor with the low-information task of verifying that measurements are within limits.

Trend analysis is a fault detection technique recommended for predicting the time frame during which a failure can be anticipated. Data is acquired on a basis of time or utilization, and compared with previous history to determine if a "trend" toward degraded performance or impending failure can be detected.

Another checkout requirement evaluated for each subsystem is periodic testing. This type of test is provided to exercise specific components at extended time intervals or prior to specific events, to assure operational integrity. In the event that a failure is detected, the periodic test will isolate to the failing Line Replaceable Unit (LRU) and accomplish recertification after a repair operation.

Calibration of specific subsystem components will be required periodically, or subsequent to a repair and/or replace operation. The techniques involved are unique to the individual component; and, in some cases, require the acquisition of operational data.

Fault isolation is required when a fault is detected. When a particular fault provides an indication that a life critical failure has occurred, the fault isolation routines are automatically initiated. If the failure does not represent an immediate danger to the vehicle occupants, the crew is notified and they will initiate the fault isolation modules at their convenience.

The basic requirements of the fault isolation function is to analyze the available information relevant to a problem, and identify the LRU which is responsible for the anomaly.

Three basic approaches to meeting this requirement were considered. These are:

- Analyze each fault as an independent problem
- Analyze each fault with a state matrix which defines the possible error states of the subsystem
- Associate each fault with a specific subsystem, and evaluate that subsystem in detail

The third approach was selected on a basis of software commonality and cost effectiveness. The complexity associated with the testing can be reduced by localization of the logic associated with the analysis of the subsystem in a unique package. The software commonality will result in reduced software development and maintenance costs, while increasing the reliability of the software.

The fault isolation software is structured modularly for compatibility with the hardware structure of the subsystem. Checkout modules evaluate the performance of a specific portion of the subsystem. A convenient division for this modular structure is at the assembly level or functional area. A program module which can determine and control the sequence in which these checkout modules are executed is also required for each subsystem.

Subsequent to fault detection, the software associated with the subsystem which is most likely to contain the error will be activated.

The subsystem software will analyze the error indication, and initiate a sequence of checkout modules to isolate the problem. If successful, the crew is notified regarding the Line Replaceable Unit (LRU) to be replaced. If an error cannot be identified, the crew is informed of the situation and has an option to execute the periodic test of the subsystem.

After a fault has been isolated, reconfiguration software restores the functional capability of the subsystem. This is most commonly accomplished by exchanging a redundant element for the failing unit, or by defining an alternate path to accomplish the required function.

The Task 2 Final Report of the basic onboard checkout techniques study provides descriptions of the software requirements, definitions and design in addition to detailed flow charts of specific checkout routines.

2

6.2. SPACE STATION SUBSYSTEM

The propulsion subsystem consists of high thrust and low thrust propellant systems. Both systems interface with the GN&C subsystem through the Data Management subsystem for operational control. The low thrust system also interfaces with the EC/LS subsystem for gases and water which are used as propellants.

The fault detection function required for the propulsion subsystem is accomplished by tables containing the parameters which must be monitored to assure subsystem performance. These tables are transferred to the Remote Data Acquisition Unit (RDAU) via the executive program. Exception monitoring is then accomplished. Figure 6-1 provides a graphic description of this function. Table 6-1 has been provided to indicate the extent of the overall fault detection requirements.

The program described by this document is required for periodic checkout and fault isolation.

Initiation of the periodic checkout function is accomplished as the result of a keyboard entry by a crew member. It is anticipated that periodic checkout will be accomplished both daily and on a tri-monthly basis with somewhat different requirements.

The fault isolation function utilizes the same software modules as the periodic checkout; however, analysis of the detected error by the sequence logic module permits selection of the appropriate module to begin the required fault isolation. If the error is not detected in the selected area, the program module provides this information and recommends that the periodic test be executed.

Subsystem calibration is performed in conjunction with the periodic test. Trend analysis is executed on a basis of varying requirements by the executive. Tables 6-2 and 6-3 have been included to provide insight to the requirements in this area.

This program meets the periodic testing and fault isolation requirements for the Propulsion Subsystem.

Since the Propulsion Subsystem consists of two independent subsystems for propulsion, the division between the high and low thrust system was used to provide definition of functional areas for the program.

Figure 6-2 provides a functional breakdown of this subsystem and indicates the associated assemblies.

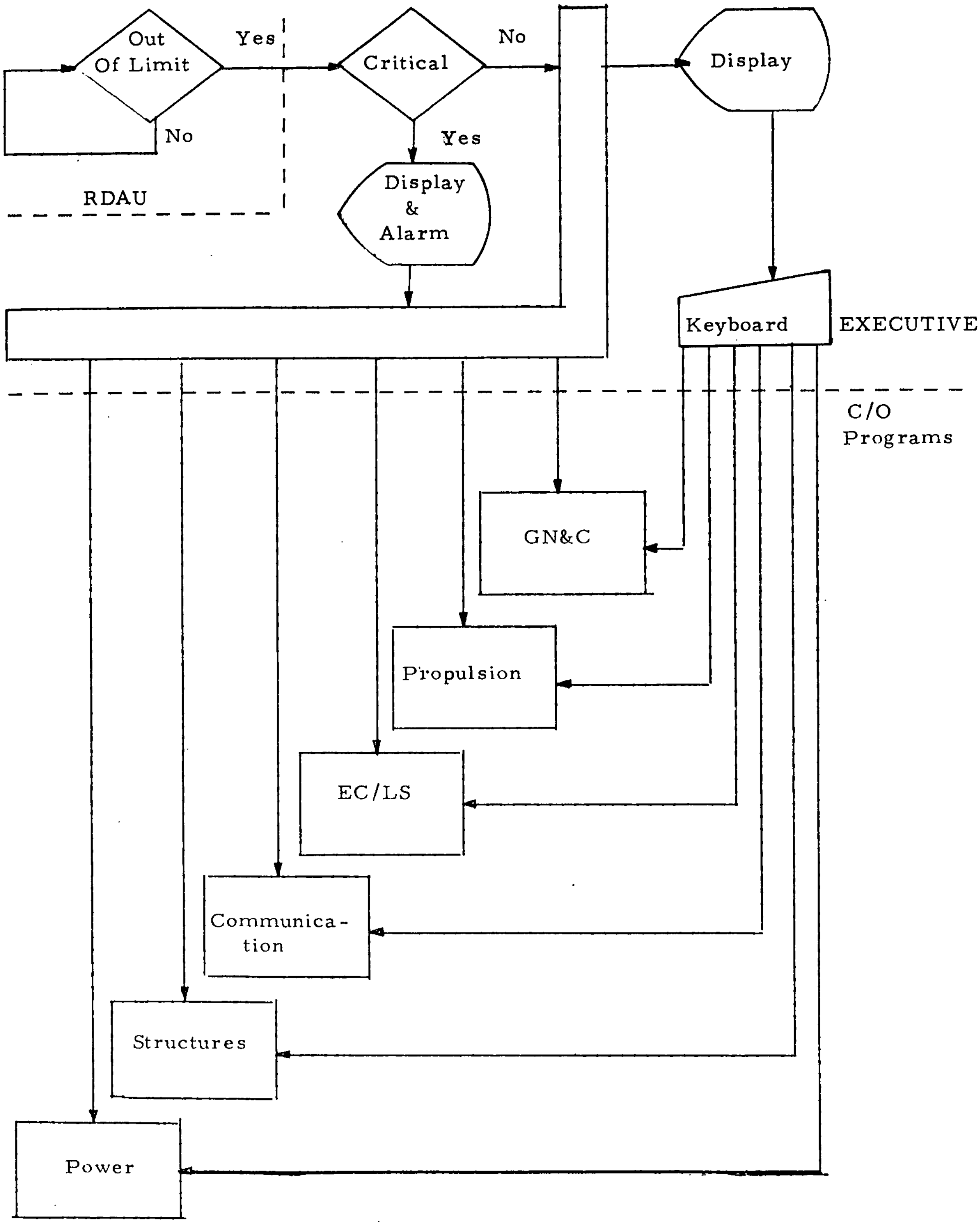


Figure 6-1. Fault Detection Logic

Table 6-1. Propulsion Subsystem Fault Detection Summary

ASSEMBLY \ SAMPLE RATE	1/Sec
Low Thrust System	
Collection/Storage Assembly	20
Water Supplement Assembly	4
Flow Control Assembly	12
Thrustor Assembly	104
Power Distribution & Control	64
High Thrust System	
Pressure Storage Assembly	8
High Pressure Manifold	2
Pressure Control Assembly	2
Low Pressure Manifold	2
Propellant Storage Assembly	28
Propellant Manifold	3
Thrustor Module	32
Purge Assembly	6
Resupply Assembly *	2
High Pressure Assembly *	8
Low Pressure Assembly *	22
Misc Temperatures	100
Total Per Second	419
Total Per Minute	25, 140
Total Per Hour	1, 508, 400
Total Per Day	36, 201, 600

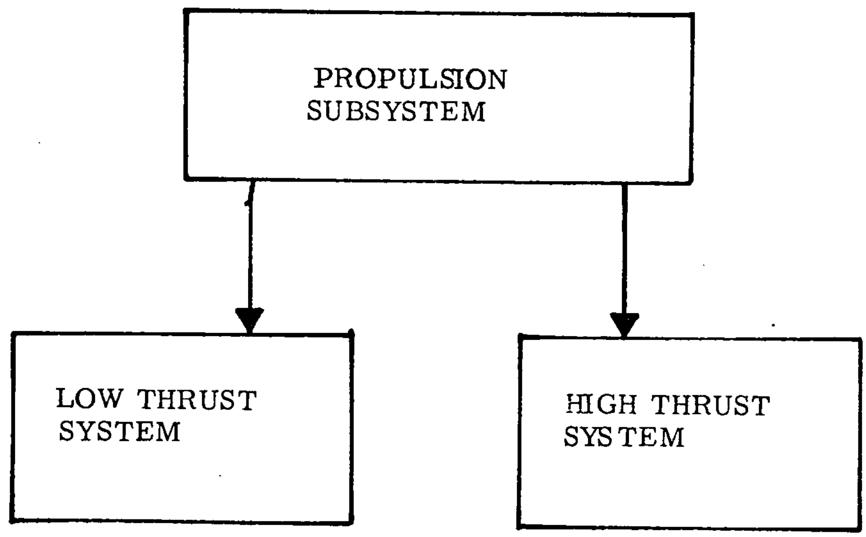
* Only during Resupply Operation

Table 6-2. Propulsion Subsystem Trend Analysis Summary

ASSEMBLY \ SAMPLE FREQUENCY	1/Day
Low Thrust System	
Collection Storage Assembly	16
High Thrust System	
Pressure Storage Assembly	8
High Pressure Manifold	2
Low Pressure Manifold	2
Propellant Storage Assembly	42
Propellant Manifold	3
Thrustor Modules	56
Purge Assembly	4
Total Per Day	133

Table 6-3. Propulsion Subsystem Calibration Summary

ASSEMBLY \ CALIBRATION FREQUENCY	1/3 Mon	1/6 Mon
Low Thrust System		
Collection Storage Assembly		24
Water Supplement Assembly		8
Flow Control Assembly		20
Thrustor Assembly		6
High Thrust System		
Pressure Storage Assembly	8	
High Pressure Manifold	2	
Pressure Control Assembly	4	
Low Pressure Manifold	2	
Propellant Storage Assembly	42	
Propellant Manifold	3	
Thrustor Modules	92	
Purge Assembly	4	
Resupply Assembly	2	
Misc Temperatures		100
TOTAL	159	158



- Collection & Storage Assembly
- Water Supplement Assembly
- Flow Control Assembly
- Thrustor Assembly
- Power Dist. & Control Assembly

- High Pressure Assembly
- Low Pressure Assembly
- Resupply Assembly
- High Pressure Manifold
- Purge Supply System
- Propellant Manifold
- Thrustor Modules
- Propellant Storage Assembly
- Low Pressure Manifold
- Pressure Control Assembly
- Pressure Storage Assembly

Figure 6-2. Propulsion Subsystem Block Diagram

6.2.1 SYSTEM REQUIREMENTS

6.2.1.1 Subsystem Definition

This program specification is based upon the subsystem definition which is available as a result of this study contract. Some test points in this subsystem are defined at the assembly level; and consequently, every failure which is detected cannot currently be identified with an LRU. Also, the correlation between the assembly test points and the LRUs is not always apparent.

6.2.1.2 Collection Storage Assembly

The algorithm required to compute gas level (mass) in the storage bottles, based upon the temperature and pressure, has not been defined. A straightforward application of Boyle's and Charles' Laws is expected.

6.2.1.3 Trend Analysis and Calibration Constants

The algorithms required for trend analysis and the calculation of calibration constants have not been defined, and could significantly impact the sizing estimates. A least-squares fit to a best straight line is recommended.

6.2.1.4 Miscellaneous Temperature

The placement of the 100 miscellaneous temperature sensors, which are defined for the subsystem, has been assumed.

6.2.1.5 Fault Detection

The operational program is responsible for maintaining the proper test points in the RDAU memory. This selection is dependent upon whether the storage assemblies are being resupplied, or the subsystem is in a "ready to fire" status.

6.2.2 OPERATIONAL REQUIREMENTS

This program specification defines specific operational requirements for automated checkout of the Space Station Propulsion Subsystem. The sequence of testing attempts to examine the least dependent functional groups first.

6.2.2.1 Sequence Logic Module

This software module is used to select the appropriate sequence of program modules to be executed in the event an error is detected in this subsystem. It also provides the sequencing required for both the daily and tri-monthly periodic tests.

This module provides the entry points for the periodic and fault isolation testing. In the event that a fault is detected, the failing test point will also be identified to this module. The only outputs from this module are the displays associated with the progress of the testing.

This module determines whether fault isolation or periodic testing is to be accomplished. In the event that fault isolation is required, the detected error is isolated to an assembly. If the program is unable to isolate an error in the selected and associated assemblies, a message is presented to the operator recommending execution of the periodic test.

When an error is detected in the Collection/Storage Assembly, it is examined; and if it was the bottle pressure or relief valve, the isolation valve is closed prior to execution of the Collection/Storage Assembly checkout module. If the detected error was the upstream pump flow, the CO_2/CH_4 flow from the EC/LS Subsystem is verified prior to execution of the Collection/Storage Assembly checkout module.

If this checkout module fails to isolate an error and the problem was detected in the propellant control valves, the checkout module for the Power Distribution and Control Assembly is executed.

When an error is detected in the Water Supplement Assembly, a check is accomplished to determine if a bottle pressure problem exists. If so, the Collection/Storage Checkout module is executed prior to the Water Supplement Assembly Checkout module to assure the current CO_2 pressure level.

The detection of an error in the Flow Control Assembly associated with the regulator requires identification of the CO_2/CH_4 or H_2O line. In this instance, the Collection/Storage Assembly checkout module, or Water Supplement Assembly checkout module, is executed to insure an adequate supply of propellant. The Flow Control Assembly checkout module is then executed to isolate the problem.

The occurrence of a module manifold pressure problem in the Thruster Assembly results in the execution of the Flow Control Assembly checkout module prior to executing the Thrustor Assembly checkout module. This assures the supply of propellants to the Thrustor Assembly. If the problem cannot be isolated, and the detected error was associated with the thrustor control valve, a final check is accomplished by executing the Power Distribution and Control Checkout module.

The occurrence of an error in the Power Distribution and Control Assembly results in execution of the checkout module for this assembly.

Errors detected in the majority of the high pressure system assemblies result in execution of the associated checkout module. In the instance of failure of the high pressure manifold, propellant manifold, and the propellant storage assembly, the program must determine if the system is in the resupply or "ready to fire" configuration in order to select the proper sequence of module execution.

6.2.2.2 Collection/Storage Assembly Checkout Module

This assembly takes the bio-waste gases (CO_2 and CH_4) from the EC/LS Subsystem and compression pumps them to the storage supply or to the flow control assembly. The gases may be stored separately or mix values can be used to combine them.

The inputs associated with this module are the test points on the assembly. The outputs are the normal operational messages indicating out-of-tolerance situations, and the progress of testing.

The program module which assesses the status of this assembly meets the requirements for fault isolation, and both daily and tri-monthly periodic testing. This module assumes that the supply of CO_2 and CH_4 gases from the EC/LS Subsystem has been verified prior to execution.

The general program flow checks the bottle, isolation valves, and propellant control valves. The fault isolation module tests only the lines (CO_2 and CH_4) in which an error was detected; but the periodic test checks all loops in both assemblies. The last components examined are the mix values. The periodic tests include all fault isolation sequences, and additional tests in the area of valve control, trend analysis, and calibration.

The daily periodic test computes the level of gas in both storage bottles based upon temperature and pressure data. This information is then transferred to the data base for operational purposes.

This routine also uses the average of upstream and downstream pump flow rates for comparison with the average of the readings from the previous ten days. If the delta between these afterages exceeds a predefined limit, the operator is notified.

The tri-monthly periodic check exercises both the propellant control and isolation valves. These valves are only exercised in the fault isolation and daily periodic test when a positional error is detected.

The tri-monthly logic computes calibration constants for the storage bottles, high and low pressure manifold temperature, and high and low manifold pressure. This data is also used to accomplish pump leak checks.

6.2.2.3 Other Software Modules

The two foregoing modules should suffice as examples. A more complete discussion is included in the Task 2 Final Report.

6.2.3 INTERFACE REQUIREMENTS

This program must interface with the Master Executive, the OCS executive, and the propulsion subsystem hardware. The propulsion subsystem must also interface with the following subsystems:

- Environmental Control/Life Support
- Power
- Guidance, Navigation and Control
- Data Management

The following interface diagrams referenced are in Appendix F of the Task 2 Final Report.

The interface between the propulsion and other subsystems is depicted in Figure 3-17 (Appendix F). Figure 3-18 (Appendix F) diagrams the assembly interfaces in the Low Thrust Subsystem. Figures 3-19 through 3-23 (Appendix F) provide detailed information regarding the Low Thrust Assemblies.

Figure 3-24 (Appendix F) represents the interface between the assemblies in the High Thrust propulsion system. Figures 3-25 and 3-35 (Appendix F) provide detailed information regarding the high thrust assemblies.

The operator is required to communicate with the program to accomplish the desired function. Specifically, the operator must initiate the program using the EXECUTE system communications element. The program may be terminated prior to completion by using the system communication function.

In addition, when errors are detected, the operator is provided with options to control program execution sequence. These options are referred to as GO-NO GO options and permit the operator to restart the LRU which failed, resume the program execution, or to terminate program execution.

Section 7

MAINTENANCE

There are two aspects of maintenance which entered into the basic study. Basic maintenance concepts were provided as part of the baseline resulting from the Phase B Space Station study; they are discussed in subsection 7.1 below. Additionally, one of the study tasks was aimed at implementation of an onboard electronics maintenance capability. The results of that task are summarized in subsection 7.2.

7.1 BASELINE MAINTENANCE CONCEPTS

Maintenance concepts defined for Space Station subsystems are intended to facilitate their preservation or restoration to an operational state with a minimum of time, skill, and resources within the planned environment.

7.1.1 GENERAL SPACE STATION MAINTENANCE POLICY

It is a Space Station objective that all elements be designed for a complete replacement maintenance capability unless maintainability design significantly decreases program or system reliability. This objective applies to all subsystems wherever it is reasonable to anticipate that an accident, wearout, or other failure phenomenon will significantly degrade a required function. Estimates of mean-time-between-failure, or accident/failure probability, are not accepted as prima facie evidence to eliminate a particular requirement for maintenance. Should the accident/failure probability be finite, the hardware is to be designed for replacement if it is reasonable and practical to do so.

As a design objective, no routine or planned maintenance shall require use of a pressure suit [either EVA or internal vehicular activity (IVA)] . Where manual operations in a shirtsleeve environment are impractical, remote control means of affecting such maintenance or repairs should be examined. However, EVA (or pressure suit IVA) is allowable where no other solution is reasonable, such as maintenance of external equipment.

Time dependency shall be eliminated as a factor of emergency action insofar as it is reasonable and practical to do so. This includes all program aspects of equipment, operations, and procedures which influence crew actions. When time cannot be eliminated as a factor of emergency action, a crew convenience period of 5 minutes is established as the minimum objective. The purpose of the convenience period is to provide sufficient time for deliberate, prudent, and unhurried action.

7.1.2 ONBOARD MAINTENANCE FACILITY CONCEPTS

In addition to OCS/DMS capabilities, other onboard maintenance support facilities provided on the Space Station include:

- Special tools for mission-survival contingency repairs such as soldering, metal cutting, and drilling, as determined from contingency maintenance analyses, although repairs of this type are not considered routine maintenance methods.
- Protective clothing or protective work areas for planned hazardous maintenance tasks (such as those involving fuels, etc.).
- Automated maintenance procedures and stock location data for both scheduled and unscheduled maintenance and repair activities.
- Real-time ground communication of the detailed procedures, update data, and procedures not carried onboard.
- Onboard cleanroom-type conditions by "glove box" facilities compatible with the level at which this capability is found to be required.
- Maintenance support stockrooms or stowage facilities for spares located in an area that provides for ease of inventory control and ready accessibility to docking locations or transfer passages.

7.1.3 SUBSYSTEM MAINTENANCE CONCEPTS

Space Station subsystems utilize modular concepts in design and emplacement of subsystem elements. Subsystem modularity enhances man's ability to maintain, repair, and replace elements of subsystems in orbit. Providing an effective onboard repair capability is essential in supporting the Space Station's ten-year life span since complete reliance on redundancy to achieve the long life is not feasible. The need for a repair capability, in turn, requires that a malfunction be isolated to at least its in-place remove-and-replace level. The level of fault isolation is keyed to the LRU, which is the smallest modular unit suitable for replacement. The identification of subsystem LRUs is addressed as a separate, but interdependent, part of the Onboard Checkout Study.

Specific subsystem maintenance concepts, of course, depend upon examination of the subsystems. These concepts are discussed in subsequent subparagraphs. General subsystem-related maintenance guidelines that have been established for the Space Station are:

- It is an objective to design so that EVA is not required. However, EVA may be used to accomplish maintenance/repair when no other solution is reasonable.

- Subsystems will be repaired in an in-place configuration at a level that is acceptable for safety and handling, and that can be fault-isolated and reverified by the integrated OCS/DMS. This level of maintenance is referred to as line maintenance and the module replaced to effect the repair is the LRU.

- A limited bench-level fault isolation capability will be provided on the Space Station, but is only intended for contingency (recovery of lost essential functions beyond the planned spares level) or for development purposes. Limited bench-level support is also provided in the form of standard measurement capabilities which are used primarily to reduce the amount of special test equipment required.

- Subsystem elements, wherever practical, will be replaced only at failure or wearout. Limited-life items that fail with time in a manner that can be defined by analysis and test will be allowed to operate until they have reached a predetermined level of deteriorated performance prior to replacement. Where subsystem downtimes for replacement or repair exceed desirable downtimes, the subsystem will include backup (redundant) operational capability to permit maintenance. Expendable items (filters, etc.) will be replaced on a preplanned, scheduled basis.

7.2 ONBOARD ELECTRONIC MAINTENANCE (STUDY TASK 3)

The objective of this task was to generate recommendations of supporting research and technology activities leading to implementation of a manned electronics maintenance facility for the Space Station. Early in the task it became apparent that attention could not be confined to a central maintenance facility; it was necessary to refocus the task to address implementation of an on-board maintenance capability encompassing in-place as well as centralized maintenance activities. The critical questions are the following:

- What is the optimum allocation of onboard maintenance functions between in-place and centralized maintenance facility locations?

- What is the optimum level of onboard repair (i.e., to line-replaceable unit, subassembly or module, piece part, or circuit element)?

7.2.1 MAINTENANCE CYCLE

In order to place the task in the proper context, a generalized Space Station electronic maintenance cycle is depicted in Figure 7-1.

A convenient place to enter the cycle is with detection of a fault ("In-Place Maintenance" block). The fault is isolated to a Line Replaceable Unit (LRU). The affected subsystem is restored to full capability by replacing the failed LRU with an operable one from spares storage.

The failed LRU is taken to a maintenance facility (assumed for the moment to have a fixed location in the Space Station) where it is first classified as repairable or non-repairable. Classifications will likely be predetermined, and a listing should be retained in the Data Management Subsystem. If the LRU is non-repairable, it is placed in segregated storage. If the LRU is repairable on board, the fault is further isolated to the failed Shop Replaceable Assembly (SRA). The LRU is then repaired by replacing the failed SRA with one from spares storage. The repaired LRU is then calibrated (if necessary), and its operation verified before it is placed in spares storage.

Logistics requirements (replacement LRUs and SRAs needed) are transmitted to ground-based logistics support functions by RF communications and/or Space Shuttle. Failed units are taken away from and replacement units are delivered to the Space Station by the Space Shuttle.

7.2.2 SUMMARY OF RESULTS

The study confirmed and emphasized the necessity of onboard maintenance for any manned mission of any complexity and duration measured in months (up to 10 years for Space Station). Formulation of recommendations for implementing such a capability required consideration of other topics first, and achievement of certain interim results. The principal conclusions of this study task are summarized below. The analyses leading to them are explained in the Task 3 Final Report.

- Prior studies and developments of in-space maintenance have emphasized justification of first-level (in-place) maintenance, fasteners, and tools for space application and human factors criteria. Much less attention has been devoted to test equipment, maintenance training, or definition of shop level maintenance requirements.

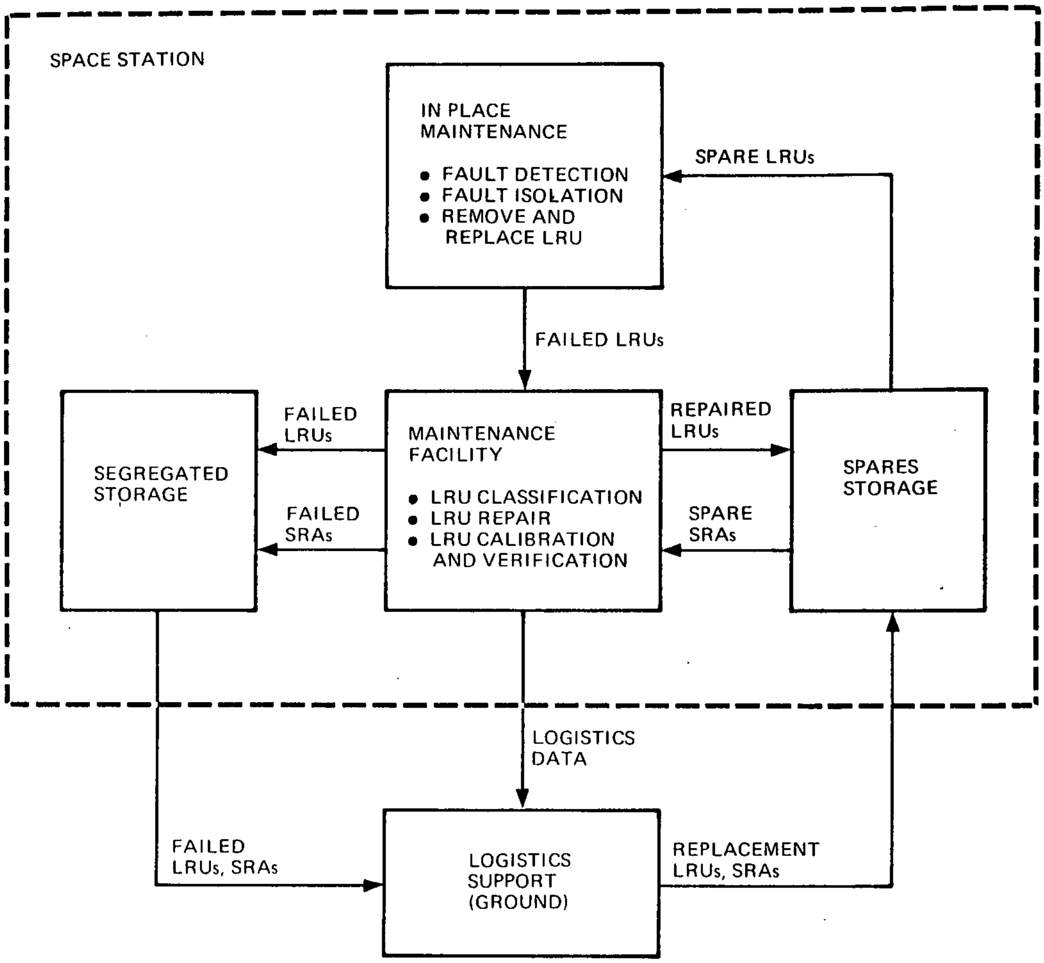


Figure 7-1. Space Station Maintenance Cycle

- The baseline subsystem descriptions, checkout requirements analysis, and software requirements analysis indicate that approximately 60 percent of all faults (over a long period) can be isolated to the failed LRU automatically under software control, without crew intervention. In an additional 27 percent of failure cases, fault isolation to one LRU can be achieved by the crew using the onboard Data Management System as a tool. In the remaining failure cases, additional fault isolation capabilities are needed. This is a good result for a "first iteration" and can probably be improved considerably with a modest effort to modify stimulus and measurement provisions.

- Crew involvement in scheduled and unscheduled maintenance (including participation in fault isolation) is estimated to average 7.2 manhours per week over the total mission time. This estimate is most sensitive to equipment reliability and levels at which onboard repair is performed. It is affected little by the efficiency of automated fault isolation under control of the Data Management Subsystem (DMS).

- The recommended approach to maintenance in the baseline Space Station is in-place removal and replacement of LRUs, without attempts to repair LRUs onboard, if the resupply interval is less than nine months. Onboard spares should be LRUs.

- For long resupply intervals or non-resupplied missions (as in a manned interplanetary mission), in-place maintenance should be by removal and replacement of LRUs. Repair of LRUs should be by removal and replacement of Shop Replaceable Assemblies (SRAs). Onboard spares should be SRAs.

- The Earth-orbital Space Station should include provision for development of onboard maintenance capability and techniques applicable to long duration non-resupplied missions and/or the larger, more complex Space Base.

- The baseline subsystem descriptions are at such a level of detail that precise specification of onboard tools and test equipment is neither feasible nor desirable. Anticipated needs identified qualitatively in the study are: (1) a portable test module to supplement software fault isolation as well as to assist mechanical adjustments and calibrator, (2) hand tools for removal and replacement of electronic assemblies, (3) devices for transporting and positioning spare assemblies, and (4) a central maintenance/repair bench.

- Several tasks have been identified and recommended for future performance, as part of a system study/design program or as separate supporting research and technology tasks. The principal ones deal with (1) development of a portable test assembly, (2) development of a repair/test bench with special provisions for small parts retention and for debris collection, (3) design for accessibility of test points and subassemblies, and (4) devices for transporting equipment within the Space Station.

The foregoing conclusions apply to the Modular Space Station as well as the 33-foot diameter, four-deck configuration.

The results of the study rest upon several assumptions and estimates, derived wherever possible from related experience. The results are not sensitive to small variations of the assumed or estimated values, except for equipment failure rates, which are most influential. Furthermore, it has not been practicable to pursue all trade analyses to include all relevant factors. Nevertheless, the study has generated valid insights into Space Station onboard maintenance and useful visibility of the path to implementation of that capability.